راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی

غلامرضا شاه محمدی[1]

تاریخ دریافت: ۹۵/۸/۱۶ تاریخ پذیرش نهایی: ۹۵/۱۲/۱۰

فصلنامه‌ی مطالعات راهبردی ناجا/ سال اول / شماره دوم - زمستان ۱۳۹۵

چکیده

فضای مجازی به دلیل ویژگی‌های خاص مانند گمنامی و سهولت ارتباط، محملی برای انواع آسیب‌ها و جرایم است و با گذشت زمان بر حجم آسیب‌ها و جرایم این فضا افزوده می‌شود. فضای مجازی امکان آسیب‌رسانی به دیگران و آسیب دیدن را توامان دارد؛ بنابراین پرداختن به مقوله پیشگیری از آسیب‌های مختلف این فضا که گستره تأثیر آن همه قشرهای جامعه را دربرمی‌گیرد، امری ضروری و اجتناب‌ناپذیر است. بررسی تحقیقات انجام‌شده در حوزه پیشگیری از آسیب‌های فضای مجازی نشان می‌دهد که در این حوزه تحقیق زیادی انجام نشده است.

زمینه و هدف: هدف این تحقیق ارائه راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی است. در این تحقیق با مطالعات گسترده کتابخانه‌ای و تجارب محقق در حوزه فناوری اطلاعات، تدابیری در قالب راهبردهای پیشگیری وضعی برای جلوگیری از آسیب‌های فضای مجازی ارائه می‌شود. تحقیق حاضر از نظر هدف از نوع کاربردی و از نظر ماهیت از نوع پیمایشی است. در این تحقیق از شیوه کتابخانه‌ای و میدانی استفاده شد. ابزار گردآوری داده‌ها پرسشنامه محقق‌ساخته است

روش: برای تحلیل داده‌ها از روش‌های آمار توصیفی و استنباطی استفاده شد.

یافته‌ها: در زمینه راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی، ابعاد حذف توجیه‌کننده‌ها، کاهش منافع حاصل از جرم، افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم و افزایش خطرهای مد نظر برای ارتکاب جرم به ترتیب بالاترین تا پایین‌ترین میانگین رتبه‌ای تأثیر در پیشگیری از آسیب‌های فضای مجازی را دارند. مهم‌ترین نتیجه این تحقیق، استخراج تدابیری در قالب راهبردهای پیشگیری وضعی برای جلوگیری از آسیب‌های فضای مجازی است که استفاده از آنها می‌تواند تأثیر زیادی در پیشگیری از آسیب‌های فضای مجازی داشته باشد.

کلید واژه‌ها

آسیب‌های فضای مجازی، پیشگیری وضعی، فضای سایبر

---

۱ . استادیار گروه فناوری اطلاعات دانشگاه علوم انتظامی امین.

مقدمه

فضای مجازی محیطی مشتمل بر شبکه‌های رایانه‌ای، رسانه‌های ارتباطی و کاربرانی است که به تبادل داده‌ها و اطلاعات می‌پردازند و هر کس مشغول کار و تأمین نیازها و علایق خویش است. این فضا باعث کوتاه شدن فاصله‌ها و استقلال از مکان شده است که بارزترین تفاوت دنیای واقعی و فضای مجازی است؛ زیرا در دنیای واقعی انسان‌ها در طول زمان و در چارچوب مکان محصورند و محدوده فعالیت‌هایشان متأثر از این واقعیات است؛ اما در دنیای مجازی با استفاده از فناوری‌های نوین ارتباطی و رایانه‌ها نقاط ضعف انسان شامل سرعت، دقت، حافظه و خستگی و مشکل جوامع کاری که همانا زمان، هزینه، نیروی انسانی و محدودیت‌های جغرافیایی است، برطرف می‌شود و با سرعتی نزدیک به سرعت نور خواسته‌ها و پاسخ‌ها به مقصد و مبدأ انتقال می‌یابد. در هر حال، فضای مجازی در هر تعبیری و با هر تعریفی، قلمرویی وسیع، بدیع و بکر است که برای ساکنان خود امکانات، آزادی‌ها، فرصت‌ها، دلهره‌ها، آسیب‌ها و محدودیت‌های تازه‌ای همراه دارد.

به تبع تغییرات ناشی از فناوری اطلاعات، زندگی بشر به فضای جدیدی منتقل می‌شود یا در حال انتقال است؛ به همین علت جرایم در اجتماع شکل جدیدی می‌یابد و به روش‌های جدیدی برای پیشگیری و کشف نیازمند است. زندگی جدید، قوانین و مقررات اجتماعی جدیدی در پی خواهد داشت که قوانین کشورهای مختلف برای مقابله با جرایم فضای مجازی از جمله این قوانین است. در فضای جدید زندگی، پلیس نقشی متفاوت از گذشته دارد و مراقبت از خیابان مانع ارتکاب و کشف جرم نمی‌شود.

فضای مجازی کارکردهای آشکار فراوانی به نمایش گذاشته و زندگی اجتماعی و فردی بشر را دچار دگرگونی کرده است. از طرف دیگر، بخش مهمی از کارکردهای پنهان فضای مجازی (پول‌شویی، هرزه‌نگاری، جاسوسی، شنود، خرابکاری، کلاهبرداری، جعل، سرقت، قاچاق، اخاذی و انواع دیگر بزه‌های اجتماعی) در راستای مأموریت‌های پلیسی است و موجب اقدامات پلیسی در جهان می‌شود.

فضای مجازی با توجه به قابلیت‌ها و ظرفیت‌های ویژه خود ماهیتی دوگانه دارد که گرچه مانند ظرفی برای تبلور اندیشه و عمل کاربران می‌نماید، مختصات و ویژگی‌های منحصر به فرد آن را نمی‌توان نادیده گرفت. به دلیل وجود همین ماهیت دوگانه، حذر از آسیب‌ها و آفت‌های فضای مجازی دشوار است. با وجود تمهیدات گوناگون و ظرفیت‌سازی گسترده‌ای که برای رشد، بالندگی و حاکمیت فرهنگ اسلامی- ایرانی در محیط مجازی

اندیشیده شده، متأسفانه در حال حاضر فضای مجازی با آسیب‌های فراوانی در حوزه اخلاق، فرهنگ، مذهب و ادب فردی و اجتماعی مواجه است؛ به گونه‌ای که پیوسته امنیت روانی والدین و اولیای امور جامعه را نسبت به ورود و استفاده کاربران جوان آسیب‌پذیر و متزلزل کرده است (الحسینی، ۱۳۹۲).

۱. اهمیت موضوع

از چالش‌های اساسی گسترش فناوری ارتباطات در جهان به خصوص کشورهای در حال توسعه در بهره‌گیری از اینترنت، آسیب‌های فرهنگی و اجتماعی است. قرار گرفتن در معرض فرهنگ‌های گوناگون، آزادی‌های زیاد در یک دورهٔ زمانی نسبتاً کوتاه و امکان دسترسی به اطلاعات غیراخلاقی گوناگون از طریق اینترنت، نمونه‌ای از این خطرهاست. در کشورهای در حال توسعه، از جمله کشور ما، به دلیل شرایط فرهنگی و اجتماعی، احتمال آسیب‌پذیری ناشی از تعامل گسترده با فرهنگ‌های دیگر زیاد است. با وجود پیشرفت‌های حاصل‌شده در سازوکارهای امنیتی و کنترلی در اینترنت، قابلیت‌های کنترلی در این‌گونه موارد کمتر مؤثر واقع می‌شوند (جلالی، ۱۳۸۲).

با توجه به انتقال بسیاری از فعالیت‌های زندگی روزمره به فضای مجازی و قابلیت‌ها و تأثیرات گسترده این فضا در انجام آسان امور، و با توجه به آمار پلیس فتا و افزایش جرایم فضای مجازی (هادیانفر، ۱۳۹۴) و آنچه در رسانه‌ها مانند صدا و سیما و روزنامه‌ها شاهد هستیم، انواع آسیب‌ها و کلاهبرداری‌ها و تهدیدها در فضای مجازی افزایش یافته است. برای مبارزه و پیشگیری از مسائل مبتلا به فضای مجازی، از آنجا که بر گستره و حجم وقوع جرایم تأثیر زیادی دارد و باعث درگیری و افزایش مسئولیت نیروی انتظامی جمهوری اسلامی ایران در مواجهه با جرم می‌شود، شناخت فضای مجازی و آسیب‌های آن و چاره‌اندیشی برای ناجا ضرورتی مهم تلقی می‌شود. این موضوع با تأسیس پلیس فتا و ایجاد مرجع رسمی کنترل و رسیدگی به جرایم سایبری اهمیتی دوچندان یافته است.

فضای مجازی با سرعت زیاد و در گستره‌ای وسیع جوامع، نهادهای اجتماعی، آموزشی، فرهنگی، مالی، سیاسی، ارتباطات اداری و حتی مناسبات بین‌المللی را به گونه‌ای مقهور خود خواهد ساخت و رویگردانی افراد و نهادها از این فضا موجب انزوا و تحمیل هزینه‌های زیاد بر آنها خواهد شد (الحسینی، ۱۳۹۲). حتی در سال ۱۳۹۱ مقام معظم رهبری فرمان تشکیل شورای عالی فضای مجازی کشور را صادر فرمودند که نشان‌دهنده توجه وافر معظم له به تأثیر شگرف این فضاست.

با گسترش استفاده از اینترنت به عنوان ابزار ورود به فضای مجازی، با توجه به: ۱. محدود نبودن فضای مجازی به مکان و زمان خاص؛ ۲. استفاده روزافزون کودکان، نوجوانان و جوانان و آحاد جامعه از این فضا؛ ۲. اشراف نداشتن خانواده‌ها بر این فضا و آسیب‌های آن؛ ۳. اندک بودن تعداد سازمان‌های مروج فرهنگ اصیل اسلامی و سازمان‌های مسئول مبارزه و پاسخگو به انواع و اقسام شبهه‌ها و اندیشه‌های الحادی و انحرافی موجود در این فضا؛ ۴. امکان حضور افراد با چهره‌های غیرواقعی و فریبکارانه و در نهایت ۵. سهولت و گستردگی ارتکاب انواع و اقسام سوءاستفاده‌ها و کلاهبرداری‌ها در این فضا، با انواع جرایم، آسیب‌ها، تهدیدها و کلاهبرداری‌ها در این فضا مواجه هستیم که تبعات ناشی از آن خیلی گسترده‌تر از فضای فیزیکی است و با توجه به آمار موجود در پلیس فتا، با گذشت زمان بر میزان وقوع انواع جرایم در فضای مجازی و آسیب‌ها افزوده می‌شود. رشد قارچ‌گونه جرایم در حوزه فضای تولید و تبادل اطلاعات کشور مانند کلاهبرداری‌های اینترنتی، جعل داده‌ها و عناوین، سرقت اطلاعات، تجاوز به حریم خصوصی اشخاص و گروه‌ها، هک و نفوذ به سامانه‌های رایانه‌ای و اینترنتی، هرزه‌نگاری و جرایم اخلاقی و برخی جرایم سازمان‌یافته اقتصادی، اجتماعی و فرهنگی ایجاب می‌کند براساس آسیب‌های فضای مجازی نسبت به استفاده از شیوه‌های مختلف پیشگیری مانند پیشگیری اجتماعی و وضعی برای مقابله با مسائل فضای مجازی اقدام کنیم (شاه‌محمدی، ۱۳۹۲).

مقام معظم رهبری بر اهمیت فضای مجازی تأکید بسیاری دارند و مدیریت آن را ضروری می‌دانند؛ به گونه‌ای که همه ارکان نظام باید نقش خاص خود را با حضوری فعال در این فضا ایفا کنند.

فضای مجازی امکان آسیب‌رسانی به دیگران و آسیب دیدن را توامان دارد و با توجه به گستره تأثیر آن که همه قشرهای جامعه را دربرمی‌گیرد، تنوع آسیب‌پذیری در حوزه‌هایی مانند فرهنگی و اجتماعی (نوری و سیدباقری، ۱۳۹۱)، روانی و روان‌شناختی (طاهری گلوندانی،۱۳۹۱)، اقتصادی (عاملی، ۱۳۹۰) و امنیتی‌ـ اطلاعاتی (طاهری گلوندانی، ۱۳۹۱)، پرداختن به مقوله پیشگیری از آسیب‌های مختلف این فضا را امری ضروری و اجتناب‌ناپذیر کرده است و بی‌توجهی به آن، هزینه‌های جبران‌ناپذیری را به جامعه تحمیل خواهد کرد.

از این رو در این تحقیق برمبنای راهبردهای پیشگیری وضعی، تدابیری برای پیشگیری از آسیب‌پذیری‌های فضای مجازی ارائه می‌شود.

هدف اصلی تحقیق: ارائه راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی

سؤال تحقیق: چه راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی وجود دارد؟

رویکرد و فرضیه: این تحقیق با رویکرد اکتشافی انجام می‌شود و فاقد فرضیه است.

۲. پیشینه تحقیق

براساس بررسی‌های انجام‌شده، تحقیقات مشابه این تحقیق عبارت‌اند از:

ـ جلالی (جلالی فراهانی، ۱۳۸۴) در مقاله ای، ضمن مرور جرایم سایبر و پیشگیری وضعی از جرم، پیشگیری وضعی از جرایم سایبر را در قالب تدابیر محدودکننده یا سلب‌کنندهٔ دسترسی، تدابیر نظارتی، تدابیر صدور مجوز و ابزار ناشناس‌کننده و رمزگذاری مطرح می‌کند. در تحقیق جلالی با وجود ارائه راهکارهایی برای پیشگیری وضعی از جرایم سایبر، نظر کارشناسان درباره این راهکارها اخذ نشده است.

ـ جلالی فراهانی (جلالی فراهانی، ۱۳۸۶) در مقاله دیگری با عنوان «پیشگیری اجتماعی از جرایم و انحرافات سایبری» ضمن اشاره به روش‌های پیشگیری اجتماعی جامعه‌مدار و رشدمدار، برای پیشگیری اجتماعی جامعه‌مدار سایبری دو حوزه عام و اختصاصی را قابل اجرا می‌داند. در حوزه عام، اشاره شده است با کدهای رفتاری می‌توان گروه‌های خاصی را که وظیفه‌ای به آنها سپرده شده است، در مقابل اعمال خود پاسخگو نگه داشت. از جمله آنها، گروه‌های مشاغل هستند که در حوزه‌های مختلف به فعالیت می‌پردازند و چون به متصدیان شبکه‌ای خود، داده‌های واجد ارزشی را واگذار کرده‌اند تا با رعایت سه اصل محرمانه بودن،[1] تمامیت[2] و دسترس‌پذیری[3] در فضای سایبر منتشر کنند، ضروری است متناسب با حرفه، نوع و میزان اطلاعات آنها و شرایط دیگر،کد رفتاری مربوط برای آنها را تدوین کنند. برای پیشگیری اجتماعی رشدمدار سایبری، راهکارهایی که بیشتر نسبت به کودکان قابلیت اجرا دارند و متولیان تربیتی و آموزشی گوناگون آنها را هدف قرار می‌دهند، مورد توجه است و اقدامات مداخله‌آمیز والدین، تدابیر همیاری همسالان، تدابیر کاربری صحیح، تدابیر کاهنده آثار سوء، تدابیر آموزشی، تدابیر الزام‌آور کار برای اینترنت و در نهایت تدابیر رسانه‌ای مطرح شده است.

ـ جلالی (جلالی، ۱۳۸۹) در مقاله خود به ابعاد مختلف نظارت همگانی پلیس و سازمان

1. Confidentiality
2. Integrity
3. Availability

مجازی پلیس در فضای مجازی به عنوان یکی از عوامل مؤثر در پیشگیری جرایم در فضای مجازی پرداخته است. هرچند دیدگاه‌های خوبی در این مقاله مطرح شده است، اما این دیدگاه‌ها اعتبارسنجی نشده است.

ـ خلیلی پور و همکارش (خلیلی‌پور و نورعلی وند،۱۳۹۱) معتقدند ویژگی‌های تهدیدهای سایبری شامل هزینه پایین ورود و سرعت بالای اقدام، گمنامی بازیگران و نداشتن قابلیت ردیابی و داشتن تأثیرگذاری شگرف، تعدد بازیگران، تأثیرگذاری شگرف، کم‌رنگ شدن نقش جغرافیا در فضای سایبری و پایین بودن احتمال تنبیه یا بازخواست اقدامات مجرمانه در فضای سایبری موجب پیدایش پدیده‌ای به نام انتشار قدرت شده که نه تنها باعث شده است دولت‌های کوچک از ظرفیت بیشتری برای اعمال قدرت در این فضا برخوردار شوند، بلکه به ورود بازیگران جدیدی مانند شرکت‌ها، گروه‌های سازمان‌یافته و افراد به معادلات قدرت جهانی انجامیده است؛ در نتیجه پدیده امنیت ملی از ابعاد مفهوم امنیت، دولت‌محوری در امنیت، بعد جغرافیایی تهدید، گستردگی آسیب‌پذیری‌ها، شیوه مقابله با تهدیدها و تعدد بازیگران در این عرصه متأثر شده است.

ـ شاه محمدی و تاهو (شاه محمدی و تاهو، ۱۳۹۳) ضمن تبیین شیوه‌های ارتکاب جرایم سایبری، به نحوه پیشگیری از آن مبتنی بر فناوری اطلاعات مشتمل بر ردیابی هویت مجازی مهاجمان، گشت فضای مجازی و کنترل و نظارت بر فضای مجازی، جمع‌آوری ادله الکترونیکی جرم و مستندسازی صحنه جرم پرداخته‌اند. جامعه آماری این تحقیق بر تأثیر این عوامل در پیشگیری از جرایم سایبری تأیید کرده است.

۳. ادبیات تحقیق

الف) فضای مجازی و ویژگی‌های آن

نخستین بار واژه فضای سایبر[1] را ویلیام گیتسون، نویسنده داستان‌های علمی‌ـ تخیلی، در کتاب نورومنسر[2] به کار برد. فضای مجازی فضا و جامعه‌ای تعریف شده است که توسط رایانه‌ها، اطلاعات و ابزارهای الکترونیکی، شبکه‌های دیجیتالی یا کاربران آن شکل می‌گیرد(Lord and Sharp, 2011: 10).

فضای سایبر[3] یا فضای مجازی در تعریف برخی نویسندگان «مجموعه‌ای از ارتباطات

1. Cyber
2. Neuromancer
3. Cyber Space

درونی انسان‌ها از طریق رایانه و وسایل مخابراتی بدون در نظر گرفتن جغرافیای فیزیکی» است؛ به عبارت دیگر «محیط الکترونیکی واقعی است که ارتباطات انسانی به شیوه‌ای سریع، فراتر از مرزهای جغرافیایی و با ابزار خاص خود، در آن، زنده و مستقیم روی می‌دهد». قید «واقعی» مانع از این تصور می‌شود که مجازی بودن این فضا به معنای غیرواقعی بودن آن است؛ زیرا در این فضا نیز همان ویژگی‌های تعاملات انسانی در دنیای خارج نظیر مسئولیت وجود دارد. فضای سایبر در واقع یک «محیط» است که ارتباطات در آن انجام می‌شود؛ نه صرفاً مجموعه‌ای از ارتباطات. از سوی دیگر، این ارتباطات گرچه ممکن است در همه حال برخط نباشند، ولی زنده، واقعی و مستقیم هستند؛ از این رو، تأثیر و تأثر زیادی در این روابط رخ می‌دهد (طارمی، ۱۳۸۷: ۱).

ب) ویژگی‌های فضای مجازی

مهم‌ترین ویژگی‌های فضای مجازی عبارت‌اند از: ۱. هزینه پایین ورود؛ ۲. گمنامی (ابراهیم‌پور کومله، ۱۳۹۱)؛ ۳. نامتقارن بودن در آسیب‌پذیری (خلیلی پور و نورعلی وند، ۱۳۹۱: ۱۹۲)؛ ۴. جهانی و فرامرزی بودن؛ ۵. دسترسی دائم و آسان به آخرین اطلاعات (عاملی، ۱۳۹۰: ۲۷)؛ ۶. جذابیت و تنوع (طارمی، ۱۳۸۷: ۲)؛ ۷. وابسته نبودن به زمان و مکان خاص (عاملی، ۱۳۹۰: ۲۷)؛ ۸. چندرسانه‌ای بودن (عاملی، ۱۳۹۰: ۲۹)؛ ۹. سهولت تعامل و تبادل اطلاعات با دیگران (ابراهیم پور کومله، ۱۳۹۱: ۳)؛ ۱۰. سرعت بالای تبادل اطلاعات و امکانات فراوان اینترنت برای افراد جامعه (ابراهیم پور کومله، ۱۳۹۱).

ج) آسیب‌های فضای مجازی

آسیب در لغت به معنای آزار، گزند، درد، صدمه و ... آمده است (عمید، ۱۳۷۹: ۳۱). آسیب‌شناسی اجتماعی، مطالعه ناهنجاری‌ها و آسیب‌های اجتماعی مانند بیکاری، اعتیاد، فقر، خودکشی، روسپی‌گری، ولگردی و گدایی همراه با علل و شیوه‌های پیشگیری و درمان آنها به انضمام مطالعه شرایط بیمارگونه و نابسامان اجتماعی است. اصطلاح آسیب‌شناسی اجتماعی شامل آن دسته از مسائل اجتماعی می‌شود که در ادراک جمعی ارائه شده و برای افراد، گروه‌ها و تمام جامعه زیان‌آور و مخرب است. آسیب اجتماعی مسئله‌ای اجتماعی است که براثر نوعی ناهنجاری، کجروی و انحراف از قوانین و ارزش‌های اجتماعی پدید می‌آید. کجروی، ناهمنوایی با هنجار یا مجموعه هنجارهای معینی است که توسط بسیاری از مردم در اجتماع پذیرفته شده است. آسیب مجازی، آسیبی دیجیتال، مبتنی بر زمان مجازی، جهانی- محلی، چندبعدی، سریع، جهانی، فراگیر، سیال و غیرعادی است (عاملی، ۱۳۹۰: ۲۸).

از پیامدهای رایانه و پس از آن اینترنت مخاطراتی است که بر جای‌جای قلمرو گسترده‌اش سایه انداخته است. چنین مخاطراتی، چنانچه مورد بی‌توجهی جامعه و حکومت قرار گیرد، بسی بزرگ و گاه جبران‌ناپذیر خواهد بود؛ زیرا آسیب‌های روانی ناشی از کاربری نادرست و خلاف قانون، موجب اختلال در رفتار افراد می‌شود و جامعه را در رسیدن به فواید بی‌شمار این فناوری نوین ناکام می‌گذارد. این اختلالات، افراد را فرسوده و ناتوان و فعالیت‌های روزمره آنان را مختل می‌کند. آسیب‌های اجتماعی و فرهنگی ناشی از آن اعضای جامعه را در رفتار فردی با خانواده و رفتار اجتماعی با سایر شهروندان و حکومت متزلزل و متأثر از فرهنگ‌های منحط بیگانه می‌کند. هنجارها و ارزش‌های متعالی جامعه رو به زوال می‌رود و احساس امنیت و آرامش از جامعه رخت برمی‌بندد. آسیب‌های سیاسی و امنیتی آن نیز موجب تضعیف اقتدار و حاکمیت دولت می‌شود و آن را در ایجاد وحدت ملی، امنیت اجتماعی و امنیت اطلاعاتی دچار چالش‌های جدی می‌کند. از طرفی آسیب‌های اقتصادی ضررهای مالی گسترده‌ای برای کاربران همراه خواهد داشت.

بر اساس آماری درباره درصد دسترسی کشورهای مختلف و استفاده کاربران از اینترنت، آمریکا و کانادا ۶۳ درصد، اروپا ۴/۲۲ درصد و استرالیا، ژاپن و نیوزلند ۴/۶ درصد از رایانه‌های متصل به اینترنت را در اختیار دارند؛ در حالی که کشورهای آسیایی و آفریقایی تنها ۹/۵ درصد از این رایانه‌ها را در خود جای داده‌اند. همچنین ۸۳ درصد کاربران اینترنت در آمریکا، ۶ درصد در اروپا، ۳ درصد در اقیانوسیه و ۸ درصد در بقیه قاره‌های دنیا قرار دارند (نجاتی حسینی، ۱۳۸۰: ۷۲).

این آمار نشان می‌دهد که بیشتر فعالیت‌ها از جمله فعالیت‌های فرهنگی را غرب انجام می‌دهد؛ به عبارت دیگر، اینترنت همراه با همه پیام‌ها و پیامدهایش که از جمله آنها رهاوردهای فرهنگی است، از غرب به شرق منتقل می‌شود و نباید پنداشت که این کار صرفاً به دلیل سیر طبیعی پیشرفت فناوری و صدور آن از سوی غرب است؛ بلکه فرهنگ‌سازی به شیوه غربی، به‌ویژه به شیوه آمریکایی، از مواردی است که غربی‌ها برای به فعلیت رساندن آن فعالیت‌های بسیاری انجام داده‌اند؛ چنان که یکی از دانشمندان پرآوازه اروپا اظهارنظر کرده بود که اکنون وقت آن رسیده است که آمریکایی شویم و منظور از جهانی شدن را همان آمریکایی شدن بدانیم. براثر رشد اینترنت و پیشرفت ارتباطات، بسیاری از سوغات‌های فرهنگی غرب به‌ویژه آمریکا، نظیر غذاهای آماده، اغذیه کنتاکی و مک دونالد و بسیاری از الگوها و مدل‌های غربی را می‌توان در بیشتر کشورهای جهان به روشنی مشاهده کرد.

آسیب در فضای فیزیکی آسیبی مبتنی بر زمان فیزیکی، محلی، تک‌بعدی، کند، محدود، راکد و عادی است؛ اما آسیب مجازی، آسیبی دیجیتال مبتنی بر زمان مجازی، جهانی‌ـ محلی، متکثر و چندبعدی، سریع، جهانی، فراگیر، سیال و غیرعادی است که در ادامه بررسی می‌شود. برخی ویژگی‌های آسیب‌های مجازی عبارت‌اند از (عاملی، ۱۳۹۰: ۴۴-۳۵):

دیجیتالی شدن آسیب: خصایص دیجیتالی شدن، قابلیت دست‌کاری، شبکه‌ای شدن، قابل فشرده و متراکم شدن و کوچک شدن است؛ بنابراین آسیب‌های مجازی نیز اجتماع‌های دیجیتالی هستند که گستره آنها نامحدود و متمایل به بی‌نهایت است و به سرعت در فضای مجازی شیوع پیدا می‌کند. غیرخطی بودن دسترسی‌ها در این فضا موجب دشواری در بحث آسیب‌ها می‌شود. آسیب دیجیتالی، آسیبی غیرخطی است و به همین دلیل کنترل آن بسیار دشوار است، زیرا امکان تحلیل و پیش‌بینی روندهای توزیع و اشاعه آن به درستی قابل برآورد نیست.

تبدیل آسیب مبتنی بر زمان فیزیکی به آسیب مبتنی بر زمان مجازی: رسانه‌ها و وسایل ارتباط جمعی که در گذشته رشدی کند و ناچیز داشتند، در عصر حاضر با تحول چشم‌گیری روبه‌رو شده‌اند؛ به گونه‌ای که عصر حاضر را «عصر اطلاعات و ارتباطات» می‌خوانند؛ ارتباط جوامع انسانی، یعنی ارتباط بین کالا، سرمایه، فرهنگ و اعتقادات که به آسانی از مرزهای جغرافیایی می‌گذرند و وارد قلمرو جوامع دیگر می‌شوند و از طرف دیگر یعنی تحول در عقاید، انگاره‌ها، پیام‌ها و ارزش‌ها.

تبدیل آسیب محلی به آسیب جهانی: آسیب‌های فضای مجازی برخلاف فضای فیزیکی، آسیب‌های جهانی است، زیرا فضای مجازی، فضایی جهانی و بی‌مرز است. آسیب‌هایی که در این فضا یا از طریق آن به وجود می‌آیند نیز آسیب‌هایی جهانی هستند. جهانی بودن آسیب مجازی نه تنها موجب گسترش سریع آن می‌شود و برای فرد در محل آثار شدیدتری دارد، بلکه برای فرهنگ و اجتماع آن فرد نیز آثار منفی همراه دارد.

تبدیل آسیب کند به آسیب سریع: آسیب‌های اجتماعی که در فضای مجازی یا از طریق فضای مجازی به وجود می‌آیند، آسیب‌های سریع هستند. سرعت بالای حرکت از جایی به جای دیگر در فضای مجازی باعث تغییرات ناگهانی شده است که خود به ایجاد مسائل و گاه آسیب‌های اساسی می‌انجامد.

تبدیل آسیب محدود به آسیب فراگیر: آسیب مجازی و آسیب‌های اجتماعی در فضای مجازی، آسیب‌های فراگیر هستند. فراگیر به این معنی که دامنه شمول آن بسیار گسترده

است. آسیب فضای فیزیکی، تنها افراد محدودی را که به جریان آسیب پیوسته‌اند، درگیر می‌کند؛ اما دامنه آسیب مجازی بسیار وسیع است. از آنجا که محدوده‌های این فضا حدود و مرزهای روشنی ندارد، افراد به صورت مداوم در موضع آسیب دیدن هستند.

از آسیب‌های فضای مجازی عبارت است از: ۱. آسیب‌های فرهنگی و اجتماعی مانند گسترش اباحه‌گری عملی (نوری و سیدباقری، ۱۳۹۱: ۴۶) و گسترش محصولات فرهنگی فرهنگ‌های منحط به‌ویژه فرهنگ غربی (طارمی، ۱۳۸۷: ۴)؛ ۲. آسیب‌های روانی و روان‌شناختی نظیر اعتیاد اینترنتی (طاهری گلوندانی، ۱۳۹۱: ۱۲)؛ ۳. آسیب‌های اقتصادی مانند قماربازی اینترنتی (عاملی، ۱۳۹۰: ۱۱۰) و اتلاف وقت و کاهش بازدهی شغلی و تحصیلی؛ ۴. آسیب‌های امنیتی- اطلاعاتی مانند جاسوسی (طاهری گلوندانی، ۱۳۹۱: ۷)؛ ۵. آسیب‌های سیاسی مانند جنگ نرم (نوری و سیدباقری، ۱۳۹۱: ۴۳) و آسیب‌های پزشکی.

۴. پیشگیری وضعی[1]

واژه پیشگیری در منابع مختلف «جلوگیری، دفع، صیانت، مانع شدن و جلو بستن» تعریف شده است (فرهنگ معین، ۱۳۶۰). اقدامات احتیاطی برای جلوگیری از اتفاقات بد و ناخواسته هم به معنای پیش‌دستی کردن، پیشی گرفتن و پیشگیری یا جلوگیری کردن، جلوی چیزی رفتن و هم به معنی آگاه کردن و هشدار دادن است (زینالی، ۱۳۸۱: ۹۹). کارکرد پیشگیری وضعی از جرم در این است که ابزار و فرصت ارتکاب جرم را از مجرم سلب می‌کند. توجه به مثلث جرم می‌تواند به درک این موضوع کمک کند. برای ارتکاب یک جرم، سه عامل باید جمع شوند. مهم‌ترین آنها که قاعدهٔ مثلث جرم را هم تشکیل می‌دهد، انگیزهٔ[2] مجرمانه است. انگیزه باعث بیدار شدن میل درونی در افراد و به تبع آن قصد[3] مجرمانه می‌شود. برای از بین بردن این عامل، ضروری است تدابیر پیشگیرانهٔ اجتماعی اتخاذ شود؛ اما اگر به هر دلیل مجرمان واجد انگیزه شدند، باید از اجتماع دو ضلع دیگر این مثلث، یعنی فرصت[4] و ابزار[5] ارتکاب جرم جلوگیری کرد. از میان این دو، سلب فرصت از مجرمان اهمیت بیشتری دارد؛ زیرا متصدیان امر هرچه بکوشند ابزارهای ارتکاب جرم را از سطح جامعه جمع‌آوری کنند، باز هم مجرمان باانگیزه خواهند توانست به آنها دست یابند؛ در عین حال نباید اهمیت جمع‌آوری

1. Situational Crime Prevention
2. Motive
3. Intention
4. Opportunity
5. Means

این ابزارها را در کاهش جرایم نادیده گرفت. به هر حال، آنچه در پیشگیری وضعی از جرایم اولویت دارد، حفظ آماج‌ها[1] و بزه‌دیدگان از تعرض مجرمان است (صفاری، ۱۳۸۰: ۲۹۲).

الف) تاریخچه پیشگیری وضعی

در دهۀ ۱۹۷۰ گروهی از دانشمندان در واحد تحقیقات وزارت کشور انگلستان در ارزیابی آمارهای جرم درباره پیشگیری، برای اولین بار اصطلاح «پیشگیری وضعی» را که صرفاً بر کاهش فرصت‌ها و موقعیت‌های ارتکاب جرم تکیه دارد، مطرح کردند. تعریف‌ها و برداشت‌های گوناگونی از پیشگیری وضعی ارائه شده است. ژرژ پیکا پیشگیری وضعی را اقدام به محدود کردن فرصت‌های ارتکاب جرم یا مشکل‌تر کردن تحقق این فرصت برای مجرمین بالقوه می‌داند (پیکا، ۱۳۷۶: ۱۰). ریموند گسن معتقد است (با توجه به تعریف‌های بیان‌شده) مصادیق و روش‌های علمی پیشگیری از جرم، مدت‌های مدیدی پیش از اینکه با این عنوان مشهور شود، وجود داشته است؛ به بیان دیگر به نظر می‌رسد پیشگیری وضعی از جرم، عنوان جدیدی است بر آنچه پلیس یا عامه آن را پیشگیری از جرم می‌نامند (گسن، ۱۳۷۰: ۱۴).

ب) اهمیت پیشگیری وضعی

وجود فرصت‌ها و مناسبت‌های ارتکاب جرم همواره یکی از عوامل مهم در بروز بزهکاری بوده و بزهکار را به ارتکاب عمل ترغیب می‌کند. تردیدی نیست که هرچه افراد، ضعف نفس بیشتری داشته باشند، در مقابل فرصت‌های ارتکاب بزه، آنگاه که منافع حاصل از جرم را سهل‌الوصول می‌بینند، دچار وسوسه بیشتری می‌شوند و زودتر به آستانه تحریک می‌رسند. برخی از جرم‌شناسان اثر فرصت‌ها در بروز بزهکاری را عاملی قطعی و تعیین‌کننده می‌دانند و معتقدند شخص مجرم به عنوان یک عامل ثابت، با ارزش صفر قلمداد می‌شود و فرصت‌های جرم به عنوان متغیرهایی که اگر ارزش مثبت داشته باشند، غنیمت شمرده می‌شوند و جرم ارتکاب می‌یابد.

ج) ویژگی‌های پیشگیری وضعی

ویژگی‌های پیشگیری وضعی عبارت‌اند از:

۱. در پیشگیری وضعی تمرکز بر جرایم خاص است؛ یعنی هر جرم اقدامات پیشگیری

1. Targets

وضعی خاص خود را دارد. مثلاً اقدامات برای سرقت وسایل اتومبیل با اقداماتی که ازکیف‌قاپی جلوگیری می‌کند، متفاوت است.

۲. پیشگیری وضعی درباره جرایم غیرعمدی مصداق ندارد، زیرا در یک لحظه به وقوع می‌پیوندد؛ اما در مورد تصادفات رانندگی، نصب سرعت‌گیر یا دوربین در بزرگراه‌ها از تدابیر پیشگیری وضعی غیرمستقیم است.

۳. پیشگیری وضعی بر محیط، انتخاب معقول، سبک زندگی و فعالیت روزمره متمرکز است. مثلاً روشنایی کوچه‌ها و خیابان‌های تاریک، فرصت ارتکاب جرم را کاهش می‌دهد. اقداماتی مانند کشیدن نرده یا حفاظ، مانع دسترسی آسان به آماج جرم است. جلوگیری از خرید و فروش اموال مسروقه یا جرم‌انگاری پول‌شویی سبب قطع رابطه پول با منشأ مجرمانه و خطرساز کردن اقدام مجرمانه می‌شود.

۵. مبانی نظری پیشگیری وضعی

اولین کسی که به رابطه میان جرم و محیط فیزیکی اشاره کرد «وود» بود که اعتقاد داشت پیشرفت در امر ساختمان‌سازی موجب ایجاد موانع و محدودیت‌هایی در روابط ساکنان می‌شود. نظریات وود، اسکار نیومن را به مطرح کردن نظریهٔ «فضای قابل دفاع» ترغیب کرد. نیومن معتقد بود که تغییرات حاصل در شکل و نقشهٔ محیط، قادر است گرایش‌ها و نگرش‌های پنهان ساکنان آپارتمان‌ها را در حفظ حریم‌شان آشکار کند و آنها را به پیش گرفتن رفتارهای مناسبی برای مراقبت از حقوق و اموال‌شان وادارد. این قبیل رفتارها به‌مرور زمان و براثر تکرار، جزئی از فعالیت‌ها و عادات روزمره می‌شوند و می‌توانند به عنوان عامل مهمی در برابر رفتارهای ضد اجتماعی عمل کنند.

دومین نسل از نظریه‌پردازان پیشگیری محیطی در مدل‌های پیشگیری از جرم، متغیرهای اجتماعی و فرهنگی را به هم پیوند زدند و تئوری فضای قابل دفاع را در قالب یک طرح ابتکاری مهم با عنوان «پیشگیری از جرم از طریق طراحی محیطی« آزمایش کردند. این نظریه را به جفری نسبت می‌دهند. اساسی‌ترین اصول این نظریه را «فرصت، هدف، ریسک و تلاش» تشکیل می‌دهد؛ یعنی فرصت ارتکاب جرم تابعی است از یک هدف، خطر، تلاش و سود. هنگامی که خطر ارتکاب جرم از منافع حاصل از آن بیشتر باشد، جرم تقلیل می‌یابد. هدف نهایی این طرح تقلیل وقوع جرم از طریق بهبود کیفیت زندگی افراد ساکن یک محله است. دانشمندانی که پیرو این نظریه هستند معتقد به ایجاد تغییرات در محیط

فیزیکی و اجتماعی، براساس چهار اصل پیشگیری از جرم هستند که عبارت‌اند از: کنترل دسترسی، مراقبت، حمایت از اقدامات ایمنی و تقلیل انگیزه‌ها برای کاهش ارتکاب جرایم.

نظریه دیگر، نظریه انتخاب معقول است که برگرفته از تحلیل اقتصادی از جرم است. طبق این نظریه، بزهکار بالقوه انسان متعارفی فرض می‌شود که در پی کسب سود از طریق انجام عمل مجرمانه است؛ بنابراین معمولاً گزینه‌ای را انتخاب می‌کند که منفعت بیشتری دربرداشته باشد. این نظریه از دیدگاه «بنتام» گرفته شده است. یکی از نقاط ضعف این نظریه این است که بزهکاران اتفاقی و آنی و بزهکار مختل المشاعر و همچنین بزهکاران معتاد و ولگرد را شامل نمی‌شود؛ زیرا مرتکبان آن به دنبال سود خاصی نیستند، بلکه منش و رفتار فرد، او را به اعتیاد یا ولگردی می‌کشاند. نظریه فعالیت روزمره نیز معتقد است برای وقوع یک جرم، سه عنصرِ بزهکار بالقوهٔ با انگیزه، بزه‌دیده با هدف مناسب و فقدان یک محافظ توانمند و کارامد، بایَد در یک زمان و مکان با یکدیگر تلاقی کنند؛ یعنی ارزش، بی‌کنشی، حجم و دسترسی؛ مثلاً اشیای با حجم کم و ارزش زیاد که همه کس به آنها دسترسی ندارند و به آسانی قابلیت جابه‌جایی دارند، اهداف مطلوب در جرایم مالی هستند (پیز، ۱۳۸۳: ۱۲۹).

نظریهٔ «سبک زندگی» هم که به بررسی مؤلفه‌های مربوط به بزه‌دیدگی شخصی می‌پردازد، ارتباط نزدیکی با نظریه فعالیت روزمره دارد و فعالیت روزمره چه در محل کار و چه در اوقات فراغت را لحاظ می‌کند. براساس این نظریه، الگوهای عملکرد یا شیوهٔ زندگی اشخاص بر احتمال بزه‌دیدگی آنها تأثیر می‌گذارد. در واقع، سبک زندگی بیان می‌کند که احتمال قربانی شدن در یک جرم با میزان قرارگیری فرد در مکان‌ها و موقعیت‌های پرخطر بیشتر می‌شود. نظریه‌های فعالیت روزمره و سبک زندگی تفاوت چندانی با هم ندارند و هر دو گزینش بزهکاری را مد نظر قرار می‌دهند؛ بنابراین از ادغام این دو نظریه می‌توان نظریه فعالیت و سبک زندگی را ارائه کرد.

الف) مزایای پیشگیری وضعی

پیشگیری وضعی نیازمند مشارکت افراد جامعه است. اعضای جامعه با مراقبت از خود و اموال خود و دیگران، در تحریک نکردن دیگران و رعایت احتیاط و ایجاد موانع فیزیکی در پیشگیری وضعی از جرم مشارکت می‌کنند. درباره جرایم بدون قربانی مانند خودکشی، اعتیاد، ولگردی، تکدی‌گری و روسپی‌گری نیز می‌توان با ایجاد محدودیت از ارتکاب جرم

آنها جلوگیری کرد. با اعمال شیوه‌های پیشگیری وضعی، ارتکاب عمل مجرمانه به تأخیر می‌افتد که این عاملِ زمان ممکن است در بسیاری موارد ارتکاب جرم را ناممکن سازد. از مزایای دیگر پیشگیری وضعی این است که چنانچه آماج و اهداف جرایم به سختی محافظت شوند و فرصت‌های ارتکاب جرم در سطح جامعه از بین بروند و خطر افزایش دستگیری مرتکبین نیز افزایش یابد، با ایجاد امکانات و فرصت‌های مشروع، بسیاری از مرتکبین بالقوه به کسب درآمد از راه‌های قانونی و مشروع اقدام خواهند کرد. کم‌هزینه بودن پیشگیری نیز از مزایای آن است؛ زیرا هزینهٔ این نوع پیشگیری بر عهدهٔ شهروندان است.

ب) پیشگیری وضعی و اقدامات پلیسی

همه اقدامات بازدارنده پلیس در بیشتر کشورها از طریق توجه به روش‌ها و تکنیک‌های پیشگیری وضعی انجام می‌گیرد؛ برای مثال پلیس با نصب دوربین‌های مخفی، هشداردهنده‌ها، سد کردن خیابان‌ها، تشدید قوانین و محدودیت‌های به‌کارگیری آلات و ادوات مجرمانه (مثل سلاح)،کنترل شدید ورودی‌ها و خروجی‌ها و .... می‌کوشد مانع بروز جرم شود. همه این اقدامات با هدف بالا بردن هزینه جرم، کاهش عواید جرم و تغییر انتخاب بزهکاران انجام می‌گیرد و از آنجا که بزهکاران معقولانه مرتکب جرم می‌شوند، این اقدامات باید بتواند آنان را از ارتکاب جرم منصرف کند (نجفی ابرندآبادی، ۱۳۷۵). همچنین استقرار پلیس در فضای جغرافیایی معین یا گشت‌های پلیس در مکان‌ها و محل‌های معین، پست‌های ایست و بازرسی و مواردی از این دست که معمولاً توسط نیروی انتظامی در شرایط زمانی و مکانی خاص انجام می‌گیرد، در چارچوب پیشگیری وضعی قرار دارد (نجفی ابرندآبادی، ۱۳۷۸: ۱۴۰).

ج) شیوه‌های پیشگیری وضعی

مفهوم آماج: آماج یا هدف جرم، موضوع بزه یا ابزاری است که امکان دسترسی به آن را فراهم می‌کند؛ چنان‌که جسم انسان آماج- موضوعِ حملات و جرایم علیه اشخاص است مانند قتل، ضرب و خشونت یا اسکناس‌های بانک یا دستگاه صوتی آماج- موضوعِ سرقت (برحسب اینکه سرقت متوجه پول باشد یا اشیای منقول) محسوب می‌شوند. آماج- موضوع به دو گروه مادی و معنوی نیز تقسیم می‌شود. آماج- موضوعِ مادی مواردی مانند زیورآلات را شامل می‌شود و کرامت، حیثیت، خلوت زندگی اشخاص و شرایط روحی- روانی، آماج- موضوعِ غیرمادی است (گسن، ۱۳۷۶: ۲۰). از سوی دیگر گاو صندوقی که پول در آن محفوظ

است «آماج- وسیله محسوب می‌شود که شکستن آن اجازه تصاحب پول را در سرقت توام با شکستن حرز می‌دهد. همچنین حامل کیف پول یا اوراق بهادار زمانی که مباشر حمله در معبر عمومی با هدف تصاحب محتوای کیف به وی تنه می‌زند و او را نقش بر زمین می‌کند، به آماج- وسیله تبدیل می‌شود (گسن، ریموند به نقل از پرویزی، ۷۹-۱۳۷۸). آماج یا اهداف جرم در فضای مجازی شامل اطلاعات شخصی (مشخصات فردی، پست الکترونیک، شناسه پست الکترونیک، حساب‌های شخصی بانکی)، اسناد سازمانی در قالب فایل‌ها، پوشه‌ها، عکس‌ها، فیلم‌ها، رایانه، ویندوز، برنامه‌ها، نرم‌افزارها، شبکه‌ها و سایت‌های سازمانی، وبلاگ‌ها، پایگاه‌های داده بانکی، افراد اعم از کودک، نوجوان، جوان و ... خانواده است.

کورنیش و کلارک[1] ۲۵ راهبرد پیشگیری وضعی را در قالب پنج دسته ارائه داده‌اند. این راهبردها عبارت‌اند از (Cornish and Clarck, 2003: 90):

دسته اول: راهبردهای مبتنی بر افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم

راهبردهای این دسته عبارت‌اند از: سخت کردن آماج جرم، کنترل ورودی‌ها به اماکن مختلف یا کنترل دسترسی به اماکن یا آماج جرم، تجهیزات و اهداف مربوط، کنترل خروجی‌ها، منحرف کردن بزهکاران از آماج و کنترل و ایجاد محدودیت برای استفاده از ابزارهای تسهیل‌کننده ارتکاب جرم.

ـ سخت کردن آماج جرم: در این شیوه از طریق ایجاد موانع فیزیکی، سد راه مجرمان بالقوه می‌شوند؛ مثلاً نصب قفل ایمنی روی فرمان خودرو و استفاده از شیشه سخت و نشکن روی اتاقک‌های تلفن‌های عمومی برای پیشگیری از تخریب سریع آنها و حفاظ‌های ضد سرقت.

ـ کنترل ورودی‌ها به اماکن مختلف یا کنترل دسترسی به اماکن، تجهیزات و اهداف مربوط: روش‌های کنترل دسترسی، ورود به محیط یا فضا برای دسترسی به آماج جرم را برای مجرمان بالقوه سخت‌تر می‌کند. این شیوه در طراحی‌های شهری برای کاهش ورود افراد غیرمسئول به اماکن معین به کار می‌رود. این روش در داخل ساختمان‌ها هم کاربرد دارد مانند تعبیه باجه نگهبانی در مجتمع‌های مسکونی یا استفاده از کلمه عبور و رمز رایانه برای جلوگیری از دسترسی افراد غیرمجاز به فایل‌های رایانه، نرده‌کشی اطراف حیاط یا باغ، نصب کارت شناسایی روی سینه افراد مجاز. هدف در کنترلِ دسترسی این است که از یک سو ورود به یک مکان از طریق گذر از یک فیلتر باشد تا سوءاستفاده‌کنندگان و افراد ناباب

1. Cornish & Clarck

نتوانند برای ارتکاب رفتار مجرمانه در آنجا نفوذ کنند و از سوی دیگر به لحاظ فیزیکی بتوان از آماج حمایت کرد (کوسن، ۱۳۷۹).

ـ کنترل خروجی‌ها: کنترل خروجی‌ها بدین منظور است که اگر بزهکار موفق به دسترسی به آماج جرم شد، باز هم موفق به خارج کردن آنها از موقعیت ارتکاب جرم نشود؛ مواردی مانند خروج اموال با برگ مجوز، مجوز خروج کالا، الصاق برچسب الکترونیکی کالا.

ـ تغییر جهت اعمال مجرمانه مرتکبین یا منحرف کردن بزهکاران از آماج: برخی کاربردهای پیشگیری وضعی از جرم سعی دارد مجرمین را از ارتکاب جرم منحرف کند؛ بدین نحو که از مواجه شدن مجرمین بالقوه با موقعیت یا فرصت ارتکاب جرم جلوگیری کند. در این روش که «کلارک» از آن با عنوان «هدایت مردم به مکان‌های خاص» نام می‌برد، سعی می‌شود با فراهم کردن محیطی امن زمینه‌های وقوع جرم از بین برود؛ مثلاً طراحی و ساخت استادیوم‌های فوتبال به گونه‌ای که تماشاچیان رقیب از هم جدا باشند تا از برخورد میان آنها و بروز جرایمی که ممکن است در آینده با اسلحه صورت گیرد، پیشگیری کند.

ـ کنترل و ایجاد محدودیت برای استفاده از ابزارهای تسهیل‌گر ارتکاب جرم یا کنترل ابزار جرم/سلاح‌ها: مثلاً سعی در محدود کردن دسترسی به بعضی سلاح‌های خاص دارند که ممکن است باعث ارتکاب جرم شوند. الصاق عکس روی کارت‌های اعتباری برای جلوگیری از سوءاستفاده از آن نیز با این هدف انجام می‌شود (محمد نسل، ۱۳۸۶).

دسته دوم: افزایش خطرهای مد نظر برای ارتکاب جرم

یکی دیگر از راهبردهای منصرف کردن بزهکاران از ارتکاب جرم، افزایش خطرهای ملموس ارتکاب جرم است. هر قدر خطر مترتب بر ارتکاب جرم بیشتر باشد، افراد کمتری رغبت به ارتکاب جرم خواهند داشت. این دسته از تدابیر پیشگیرانه نیز شامل پنج شیوه می‌شود: ۱. توسعه محافظت؛ ۲. نظارت طبیعی؛ ۳. کاهش گمنامی؛ ۴. نظارت به وسیله کارمندان یا استفاده از مدیران محلی در پیشگیری؛ ۵. تقویت نظارت رسمی.

ـ زیر نظر قرار دادن ورودی‌ـ خروجی در اماکن عمومی: مثل گشت مرزی، کنترل چمدان‌ها در فرودگاه‌ها و پایانه‌های مسافری (با وسایل الکترونیکی)، نصب برچسب کتابخانه روی کتاب‌ها برای شناسایی آنها هنگام خروج از طریق دستگاه‌های الکترونیکی، بازرسی ورودی‌ها و خروجی‌هایی که می‌توانند در پیشگیری از وقوع برخی جرایم سودمند باشند مثل نصب فلزیاب در ورودی‌های فرودگاه‌ها که موجب افزایش خطر دستگیری کسانی

می‌شود که قصد بردن سلاح یا مواد منفجره به داخل هواپیما را دارند.

ـ **توسعه محافظت:** در بررسی نظریهٔ فرصتِ جرم بیان می‌شود که فقدان محافظ کارامد یکی از عوامل افزایش خطر ارتکاب جرم است؛ در مقابل، تقویت محافظت از آماج بالقوه جرم موجب انصراف بزهکار بالقوه از عملی کردن تصمیم ارتکاب جرم می‌شود و حتی در صورت اقدام مرتکب نیز موجب ناکامی وی در اتمام موفقیت‌آمیز عملیات اجرایی می‌شود.

ـ **تقویت نظارت رسمی:** به نظر دنیس رزنبام، نظارت رسمی، بهترین شیوه پیشگیری وضعی از جرم است. نظارت رسمی، مراقبت کاملاً آشکار و محسوسی است که هوشیاری و نظارت و کنترل اوضاع را به بزهکاران بالقوه یادآوری می‌کند و آنها را متقاعد می‌سازد که در صورت ارتکاب جرم، شناسایی و دستگیر خواهند شد. افزایش احتمال واکنش فوری پلیس و نیروهای محافظ موجب انصراف بزهکاران بالقوه از ارتکاب جرم می‌شود. از جمله شیوه‌های این رسانه می‌توان به نصب دوربین‌های مدار بسته در نقاط معین و همچنین نصب دوربین‌های سنجش سرعت و ثبت تخلفات در جاده‌ها اشاره کرد (محمد نسل، ۱۳۸۶).

ـ **نظارت به وسیله کارمندان:** آموزش کارکنان مؤسسات عمومی و خصوصی و استفاده از آنان در برقراری یا تقویت محافظت از محیط و اموال نیز از شیوه‌های مؤثر پیشگیری وضعی است. احساس هوشیاری و کنترل اوضاع توسط کارکنان موجب انصراف و ناامیدی بسیاری از بزهکاران علاقه‌مند به ارتکاب جرم می‌شود و در صورت ارتکاب جرم نیز با واکنش حساب‌شده، موجب افزایش ضریب دستگیری مرتکبان می‌شود. بهره‌برداری از کارکنان فروشگاه‌ها، ناظرین پارک‌ها، نصب تلفن‌های عمومی سکه‌ای (کافی نت) در محل‌های زیر نظر مثل مغازه‌ها و نگهبانان پارک‌ها از مصادیق این شیوه است.

ـ **کمک گرفتن از نظارت طبیعی:** نظارت طبیعی تدبیری است که از طریق اصلاح طراحی محیطی و بهبود شرایط طبیعی موجب افزایش توانایی انسان یا تجهیزات فنی در مراقبت از یک منطقه می‌شود. طراحی/ ایجاد محیط قابل دفاع، تقویت روشنایی خیابان‌ها و مغازه‌ها و معابر با قادر ساختن ساکنان و رهگذران به مشاهده فعالیت‌های سطح خیابان از بسیاری از بزهکاری‌های شبانه جلوگیری می‌کند (رزنبام، ۱۳۷۹: ۱۵۱).

ـ **کاهش گمنامی:** کاهش گمنامی و سهولت شناسایی مرتکبانِ اقداماتِ بزهکارانه نیز از تدابیری است که خطر دستگیری پس از ارتکاب جرم را افزایش می‌دهد و از این طریق موجب انصراف بزهکاران از اجرای جرم می‌شود. صدور کارت شناسایی برای رانندگان تاکسی، الزام آنان به نصب آن روی شیشه جلوی خودرو و امکان مشاهده آن توسط مسافران

از بسیاری از جرایمی که ممکن است رانندگان تاکسی در قبال برخی مسافران مرتکب شوند، جلوگیری می‌کند.

ـ **بهره‌گیری از ابزارهای مدیریت بر مکان:** تلویزیون مدار بسته در اتوبوس‌های دو واگنه، دو خدمه برای فروشگاه غذای آماده.

دسته سوم: کاهش جاذبه آماج‌ها یا دستاوردهای مورد انتظار از جرم یا همان سود حاصل یا کاهش منافع حاصل از جرم

این دسته مبتنی بر نظریه انتخاب عقلانی و نظریه اقتصادی جرم است. مطابق این نظریه، فرد بزهکار با سنجش میزان سود و زیان حاصل، زمانی ارتکاب جرم را انتخاب می‌کند که منافع حاصل از جرم ارزشمندتر از ضررها و خطرهای ناشی از ارتکاب آن باشد. پنج شیوه زیر در این دسته جای می‌گیرند: ۱. نهان/ مخفی کردن آماج جرم؛ ۲. از دسترس خارج کردن یا جابه‌جایی و برداشتن آماج جرم؛ ۳. شناسایی یا نشانه‌گذاری اموال؛ ۴. برهم زدن بازارهای غیرقانونی؛ ۵. تضییق یا زوال یا جلوگیری یا از بین بردن منافع/سود.

یکی دیگر از راهبردهای پیشگیری وضعی که کلارک به آن می‌پردازد کاهش میزان درآمد و سود حاصل از ارتکاب جرم برای مجرمین است. این روش اشکال متنوعی دارد که عمده آنها عبارت‌اند از: حذف آماج‌های جرم، علامت‌گذاری اموال، تقلیل وسوسه‌ها و حاکم کردن قواعد خاص بازدارنده در خصوص حذف آماج‌های جرم. می‌توان گفت با حذف یک آماج که مورد توجه مجرمین است و تبدیل آن به نوع دیگری که آن خصوصیات را نداشته باشد، می‌توان برنامه‌های ارتکاب جرم را از بین برد یا کاهش داد.

ـ **برهم زدن بازارهای غیرقانونی:** برهم زدن بازار جرم نیز تحقق هدف غایی از جرم را دچار تردید جدی می‌کند و انگیزه مرتکب را تنزل می‌دهد و موجب انصراف وی از ارتکاب جرم می‌شود. کنترل سمساری‌ها و محل‌های فروش لوازم دست دوم، ساماندهی و صدور مجوز برای دست‌فروش‌های خیابانی، نظارت بر بنگاه‌های کارگشایی و کنترل بر آگهی‌های نیازمندی‌ها از رایج‌ترین شیوه‌های اجرای این تکنیک هستند.

ـ **نهان/ مخفی کردن آماج جرم:** نهان/ مخفی کردن آماج جرم، شناسایی آماج جرم و در نتیجه ارتکاب جرم را از بزهکارانی که در جست‌وجوی تعیین شکار مناسب هستند، سلب می‌کند. از مصادیق این شیوه، ممنوعیت پارک خودرو در خیابان، چاپ و انتشار کتابچه راهنمای تلفن بدون تعیین جنسیت صاحبان تلفن (برای جلوگیری از شناسایی زنان مجرد و ارتکاب جرایم جنسی روی آنان) است.

ـ از دسترس خارج کردن یا جابه‌جایی و برداشتن آماج جرم: از دسترس خارج کردن آماج جرم نیز اساساً دسترسی به آماج جرم را برای مرتکبان غیرممکن و آنان را برای ارتکاب جرم ناتوان می‌کند. استفاده از کارت تلفن به جای تلفن سکه‌ای (برای جلوگیری از سرقت سکه‌ها از قلک کنتورها و از باجه تلفن)، برداشتن ضبط خودرو، استفاده از کارت اعتباری برای تلفن عمومی نمونه‌هایی از این شیوه هستند.

ـ شناسایی اموال/ شناساندن یا نشانه‌گذاری اموال: شیوه مشخص کردن اموال به منظور تضعیف انگیزه بزهکاران، آنان را از ارتکاب جرایم علیه اموال منصرف می‌کند. از مصادیق این شیوه درج نام رستوران‌ها روی ظروف غذا، علامت‌گذاری اموال و اثاثیه ذی‌قیمت، استفاده از شماره رمز برای ورود به رایانه، درج شماره سریال روی قطعات خودرو و صدور کارت شناسایی برای وسایل خودرو نقلیه است.

ـ حذف یا کاهش جذابیت وسایل تحریک‌آمیز: مثل کاهش آثار مخرب سلاح‌ها، تمیز کردن بی‌نزاکتی‌ها از روی دیوارها، تعمیر سریع (تلفن‌های شکسته یا صندلی‌های اتوبوس) و ارائه فهرست اسامی و شماره تلفن بدون ذکر نام خانم و آقا (برای جلوگیری از شناسایی شماره تلفن‌هایی که متعلق به خانم‌هاست).

ـ تضییق یا زوال یا جلوگیری یا از بین بردن منافع/سود: از بین بردن سود ناشی از ارتکاب جرم عملاً ارتکاب جرم را به عملی لغو و بی‌نتیجه تبدیل و سرانجام مرتکب را از انجام جرم منصرف می‌کند. تعبیه کد، رمز برای به کار انداختن رادیو پخش خودرو، پاک کردن فوری دیوارنوشته‌ها و بی‌نزاکتی‌های روی دیوار از رایج‌ترین شیوه‌های این تکنیک است (محمد نسل،۱۳۸۶).

دسته چهارم: حذف بهانه‌ها یا توجیه‌کننده‌ها یا معاذیر یا از بین بردن عوامل تحریک یا تشویق فرد به ارتکاب جرم

بهانه‌ها در تکوین فرایند تصمیم‌گیری و گذار مرتکب از مرحله تصمیم به عمل نقش مهمی دارند. پنج شیوه اصلی این دسته عبارت‌اند از: ۱. برقراری/ وضع قواعد/ مقررات؛ ۲. پست راهنما؛ ۳. تحریک/ هوشیاری وجدان و آگاهی؛ ۴. تسهیل رعایت قوانین؛ ۵. کنترل مواد مخدر.

ـ برقراری/ وضع قواعد/ مقررات: با وضع مقررات می‌توان از بسیاری از زمینه‌های وقوع جرم پیشگیری کرد. اقداماتی مانند ثبت نام مسافران در هتل‌ها و قراردادهای اجاره و وضع مقررات برای مزاحمت از مصادیق معروف این شیوه است.

ـ **پست راهنما:** متوجه کردن، از درگیر شدن ناخواسته افراد در فعالیت مجرمانه پیشگیری می‌کند. تذکراتی مانند «جلوی در منازل یا محل‌های پارک ممنوع، پارک نکنید»، موارد پارک در این محل‌ها را کاهش می‌دهد.

ـ **تحریک/ هوشیاری وجدان و آگاهی:** گاهی تحریک مختصر وجدان برای کسانی که در مرز بین درستکاری و بزهکاری قرار دارند، بسیار کارساز است و یکباره فرد را درباره عملکرد خود هوشیار می‌کند. نصب تابلوهای سنجش سرعت در کنار جاده موجب کاهش سرعت رانندگان شده است.

ـ **تسهیل رعایت قوانین:** کمک به هماهنگی نیز شیوه دیگری است که عوامل حمایتی را برای سازگاری با محیط و اجتناب از جرم تقویت می‌کند. هر قدر شرایط سازگاری با هنجارها آسان‌تر باشد، ارتکاب جرم و ناهنجاری کمتر می‌شود. اقداماتی مانند سهولت ثبت و تحویل کتاب در کتابخانه‌ها و ساخت توالت عمومی از مثال‌های این شیوه است که از رفتارهای نابهنجار جلوگیری می‌کند.

ـ **کنترل مواد مخدر:** مواد مخدر از عوامل زمینه‌ساز جرم است و ممنوعیت مصرف مواد مخدر، احتمال وقوع جرم را کاهش می‌دهد.

ـ **کنترل رهاکننده‌ها:** مانند نصب تراشه‌های مخصوص روی تلویزیون و رایانه برای استفاده کنترل‌شده از آنها.

دسته پنجم: کاهش محرک‌های وضعی

ـ **کاهش سرخوردگی و فشار روحی:** صف‌بندی کارامد و خدمات مؤدبانه مانند افزایش تعداد صندلی‌ها در اماکن عمومی؛

ـ **اجتناب از مشاجره:** مانند جدا بودن هواداران تیم‌های فوتبال رقیب از هم یا تعیین کرایه تاکسی‌ها؛

ـ **کاهش تحریک احساسات عاطفی:** مانند نظارت عکس‌های مستهجن و خشونت‌آمیز یا رفتار خوب در زمین فوتبال؛

ـ **خنثی کردن فشار در گروه‌های مشابه:** مانند نه گفتن چیز خوبی است یا جدا کردن مشکل‌سازها از هم در مدرسه؛

ـ **ممانعت از تقلید:** مانند ترمیم سریع خرابکاری‌ها، تراک‌های نمایشی در تلویزیون و سانسور جزئیات شیوه کار.

د) استفاده از روش‌های پیشگیری وضعی برای پیشگیری از آسیب‌های فضای مجازی

بررسی نشان می‌دهد که از پنج دسته راهبرد پیشگیری وضعی، چهار دسته برای پیشگیری از آسیب‌های فضای مجازی هم استفاده می‌شوند. پس از جمع‌بندی روش‌های ارائه‌شده برای پیشگیری متناسب با هر دسته از روش‌های پیشگیری وضعی، جدول‌های ۱ تا ۴، دسته‌های اصلی، فرعی و روش‌های پیشنهادشده برای پیشگیری از آسیب‌های فضای مجازی برمبنای راهبردهای اصلی و فرعی را نشان می‌دهد.

جدول ۱: راهبردهای مبتنی بر افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم

دسته فرعی	مصادیق
۱. سخت کردن آماج جرم	۱. نصب دیواره آتش ویندوز در کامپیوتر ۲. نصب ویروس‌یاب و به‌روز نگه‌داشتن آن روی رایانه ۳. قرار ندادن اطلاعات شخصی و سازمانی روی رایانه متصل به اینترنت ۴. بستن پورت‌های ورودی رایانه ۵. نصب دیواره آتش در ورودی شبکه ۶. رمزگذاری روی فایل‌ها، پوشه‌ها، رایانه، ویندوز، SETUP ویندوز و تغییر منظم آنها و استفاده نکردن از مشخصات شخصی مثل سال تولد، شماره شناسنامه برای رمز ۷. استفاده نکردن از رمزهای پیش‌فرض و یکسان نبودن عنوان شناسه کاربری و رمز ۸. درج نکردن صریح آدرس ایمیل در فضای مجازی تا توسط برنامه‌ها قابل استفاده نباشد. ۹. ممنوع کردن نصب نرم‌افزارهای سازمانی روی رایانه متصل به اینترنت ۱۰. رمزگذاری مناسب برای حساب‌های کاربری (با استفاده از ترکیب حروف بزرگ و کوچک و ارقام) ۱۱. علاوه بر رمز از شناسه رنگ برای ورود به سایت‌ها استفاده شود. ۱۲. استفاده از صفحه کلید مجازی برای جلوگیری از لو رفتن رمز حساب بانکی ۱۳. درج نکردن اسم کوچک در کلوپ‌ها و سایت‌ها و شبکه‌های اجتماعی ۱۴. خارج کردن درایوهای ویندوز از حالت اشتراکی پیش‌فرض ۱۵. از دسترس خارج کردن از راه دور کامپیوترها (....Remote) ۱۶. انتقال شبکه‌ها و سایت‌های حاوی اطلاعات سازمانی یا شرکت‌ها از اینترنت به اینترنت ملی ۱۷. غیرفعال کردن GUEST سیستم ۱۸. عدم اجازه‌دهی به نرم‌افزارهای مرورگر وب برای ذخیره کردن رمز عبور

دسته فرعی	مصادیق
۲. کنترل ورودی‌ها به اماکن مختلف یا کنترل دسترسی به اماکن، تجهیزات و اهداف مربوط	۱. کارت ورود الکترونیکی- حفاظ تجهیزات ۲. انتقال اطلاعات سازمان‌های دولتی و خصوصی که مورد استفاده داخل کشور است، به شبکه ملی کشور مانند اطلاعات بانک‌ها، ثبت احوال و ... ۳. اتصال شبکه‌های سازمان‌های دولتی و خصوصی که مورد استفاده داخل کشور است، به شبکه ملی کشور. ۴. جدا کردن شبکه‌های سازمان‌های دولتی و خصوصی مورد استفاده داخل کشور از اینترنت ۵. استفاده از دیواره آتش ویندوز و شبکه ۶. اختصاص شناسه کاربری و رمز برای کاربران اینترنت دانشگاه‌ها، ادارات و ... و استفاده از نرم‌افزارهای کنترل ترافیک شبکه و تهیه نرم‌افزارهای تهیه ثبت وقایع برای بررسی سوءاستفاده و ... افراد از اینترنت و در صورت لزوم لغو مجوز استفاده آنان از اینترنت ۷. استفاده از فیلتر برای جلوگیری از ورود کودکان، نوجوانان، دانش‌آموزان، دانشجویان و کارمندان به وبلاگ‌ها، سایت، شبکه‌های اجتماعی غیرمجاز و ... ۸. فعالیت کودکان و نوجوانان با نرم‌افزارهای مناسب بررسی شود و در صورت مراجعه به سایت‌ها/ شبکه‌ها ... یا انجام اعمال ارتکاب جرم، استفاده آنها محدود شود. ۹. محدود کردن استفاده مجرمین از اینترنت: استفاده از خدمات اینترنت مبتنی بر بررسی صلاحیت باشد و در صورتی که فرد دچار جرم/ ارتکاب جرم /کلاهبرداری در فضای مجازی شد، استفاده‌اش از اینترنت لغو شود و یکی از مراکز تأیید صلاحیت، پلیس فتا باشد. ۱۰. استفاده کنترل‌شده افراد دارای سوابق مجرمیت از اینترنت ۱۱. صدور کارت عابر بانک برای افراد با سابقه کلاهبرداری باید با اخذ مجوز از مراجع ذی‌صلاح و کسب صلاحیت لازم صورت گیرد. ۱۲. با استفاده از نرم‌افزارهای ثبت وقایع و ایمیل افراد سابقه‌دار، ارتکاب اعمال مجرمانه آنها بررسی شود. ۱۳. غیر فعال کردن امکان اتصال حافظه فلاش و دیسک‌های خارجی به رایانه‌های حاوی اطلاعات سازمانی ۱۴. برداشتن درایو CD/DVD رایانه‌های حاوی اطلاعات سازمانی ۱۵. ممنوع کردن ورود DVD/CD یا فلاش به محل‌هایی که رایانه‌های حاوی اطلاعات سازمانی امکان اتصال حافظه فلاش یا DVD/CD را دارند. ۱۶. راه‌اندازی سرویس ACTIVE DIRECTORY و تعریف سیستم‌ها در یک دامنه ۱۷. نصب رمزکننده‌ها روی شبکه‌های دامنه ۱۸. استفاده از قفل‌های سخت‌افزاری برای تبادل اطلاعات یا اجرای سیستم‌ها یا نرم‌افزارها یا سامانه‌ها ۱۹. تعریف کنترل دسترسی کاربران به منابع سیستم ۲۰. محدود کردن تعداد تلاش ناموفق برای دسترسی به سیستم ۲۱. پرهیز در استفاده از نرم‌افزارهای ناشناخته برای اتصال به اینترنت ۲۲. استفاده از نرم‌افزارهای مصوب و بررسی‌شده در سطح سازمان ۲۳. عدم ورود کودکان .... به وب سایت‌ها، شبکه‌ها، وبلاگ‌ها، لینک‌ها و ... ناشناخته ۲۴. پاسخ ندادن به ایمیل‌های ناشناخته و مشکوک ۲۵. ایجاد رویه و مجوز برای ورود تجهیزات رایانه‌ای به سازمان ۲۶. ایجاد رویه استاندارد در خرید تجهیزات رایانه‌ای

دسته فرعی	مصادیق
۳. کنترل خروجی‌ها	۱. خروج با مجوز رایانه، حافظه‌های مختلف و اسناد رایانه‌ای از سازمان‌ها ۲. محدود کردن زمان خروج تجهیزات رایانه‌ای ۳. ایجاد سیاست مناسب برای از رده خارج کردن تجهیزات رایانه‌های ۴. حذف امکان اتصال هرگونه حافظه یا دستگاه خارجی حافظه‌دار به رایانه‌های متصل به اینترنت ۵. کنترل و بررسی LOG های ورود و خروج اطلاعات به سیستم‌ها ۶. ایجاد یک کنترل مناسب روی پورت‌های سوییچ شبکه که در صورت اتصال حافظه یا دستگاه‌های خارجی، با غیرفعال کردن پورت سوییچ با ایجاد آلارم یا ثبت در LOG به مدیر شبکه اطلاع‌رسانی کند. ۷. استفاده از دوربین‌های مدار بسته برای کنترل ورودها و خروج‌ها استفاده از تگ‌های RFID برای شناسایی و جلوگیری از خروج غیرمجاز تجهیزات سازمانی
۴. تغییر جهت اعمال مجرمانه مرتکبین یا منحرف کردن بزهکاران از آماج	۱. محدود کردن زمان استفاده از اینترنت کودکان، نوجوانان، جوانان و ... ۲. تنظیم برنامه‌های مفرح برای کودکان و نوجوانان تا کمتر از فضای مجازی استفاده کنند. ۳. ایجاد سایت‌ها، وبلاگ‌ها، شبکه‌های اجتماعی مجازی در زمینه امور آموزشی، فرهنگی، هنری، علمی و ... منطبق با فرهنگ اسلامی ۴. برگزاری انواع مسابقه‌ها و همایش‌های علمی و فرهنگی در فضای مجازی ۵. معرفی سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی مجازی مفید به کودکان و نوجوانان و ... ۶. اهمیت دادن به اختراعات و نوآوری‌ها و سوق دادن جوانان به آن ۷. اشتغال‌زایی برای جوانان و ... تا کمتر به ... بپردازند. ۸. استفاده از رسانه‌های تبلیغی مناسب برای اطلاع‌رسانی برنامه‌های مفید ۹. تبلیغ تأثیرات ورزش در سلامتی جسمی و روانی ۱۱. نمایش عواقب ارتکاب جرم و ... در فضای مجازی از طریق روش‌های مختلف سیما، در سایت و ... ۱۲. ایجاد و ترویج بازی‌های رایانه‌ای منطبق با فرهنگ اسلامی متناسب با سن افراد

دسته فرعی	مصادیق
۵. کنترل و ایجاد محدودیت برای استفاده از ابزارهای تسهیل ارتکاب جرم	۱. جمع‌آوری مراکز فروش رسانه‌های رایانه‌ای غیرمجاز ۲. جمع‌آوری فیلترشکن‌ها از سایت‌ها یا فیلتر کردن سایت‌های مسئله‌دار ۳. نصب عکس روی کارت‌های اعتباری بانکی (برای جلوگیری از سوءاستفاده افراد غیرمجاز) ۴. نصب فناوری لازم روی تلفن‌ها برای شناسایی تلفن‌کننده برای پیشگیری از مزاحمت‌های تلفنی ۵. استفاده از ابزار محدودکننده پهنای باند اینترنت برای مصارف مختلف خانگی، اداری و سازمانی ۶. نصب دوربین در سایت‌ها برای مشاهده استفاده کارکنان، دانشجویان و دانش‌آموزان از اینترنت ۷. قرار دادن رایانه در سایت به نحوی که در معرض دید همگان باشد. ۸. استفاده از نرم‌افزارهای تهیه ثبت وقایع و کنترل استفاده افراد از اینترنت و فضای مجازی برای کنترل سوءاستفاده و در صورت استفاده غیرمجاز یا اتصال به سایت‌ها/ شبکه‌های اجتماعی غیر مجاز و ... ابتدا تذکر و در صورت تکرار، مجوز استفاده لغو شود. ۹. کنترل رایانه‌های متصل به اینترنت در سایت و سایر محل‌ها که روی آنها نرم‌افزار فیلترشکن نصب نباشد. ۱۰. کنترل رایانه‌ها و لپ تاپ‌های موجود در خانه توسط والدین که فیلترشکن روی آنها نصب نباشد. ۱۱. ندادن شناسه کاربری ADMIN به دانش‌آموزان و دانشجویان برای نصب نرم‌افزارهای سازمانی یا فیلترشکن برای ... ۱۲. ردیابی IP، ردیابی ارسال‌کننده ایمیل مورددار از روی هدر ایمیل ۱۳. در صورت برداشتن موارد خلاف از روی اینترنت توسط کاربر، تذکر و لغو مجوز استفاده از اینترنت ۱۴. جداسازی رایانه‌های سازمانی از رایانه‌های متصل به اینترنت ۱۵. کاربران رأساً قادر به نصب نرم‌افزار روی رایانه نباشند تا احیاناً نتوانند نرم‌افزار مسئله‌دار نصب کنند. ۱۶. کنترل فقدان فیلترشکن روی رایانه متصل به اینترنت ۱۷. نداشتن امکان اتصال حافظه فلاش و خارجی به رایانه‌های سازمانی ۱۸. در صورت مواجهه با اعمال مجرمانه و خلاف شئونات در فضای مجازی موارد به پلیس فتا انعکاس شود و پلیس فتا در اسرع وقت پیگیری کند. ۱۹. ایجاد یک سایت در فضای مجازی برای رسیدگی به شکایت مردمی- کلانتری مجازی ۲۰. معرفی سایت‌های مسئله‌دار به جامعه از نظر فرهنگی ۲۱. محدود کردن ساعات استفاده از اینترنت در خانه برای فرزندان ۲۲. ممنوع کردن ورود کودکان و نوجوانان به شبکه‌های اجتماعی مجازی و سایت‌های مسئله‌دار و ناشناخته ۲۳. فیلتر کردن سایت‌ها، وبلاگ‌ها و ... مسئله‌دار و غیرمجاز
۶. کنترل ابزار/آلات جرم/ سلاح‌ها	۱. ایجاد یک رویه برای تعیین صلاحیت وب سایت‌ها، وبلاگ‌ها و ... توسط مراجع ذی‌صلاح و درج نمادی در وبلاگ، وب سایت و ... که نشان‌دهنده واجد شرایط بودن آنهاست. ۲. ایجاد گشت سایبری و فیلتر کردن سایت‌های دارای فیلترشکن و موارد مسئله‌دار ۳. کنترل و نظارت فیزیکی در سایت‌ها و ... توسط پلیس فتا و بررسی ترافیک شبکه با استفاده از نرم‌افزارهای مناسب برای کنترل شبکه و سوءاستفاده‌ها ۴. کنترل وبلاگ‌ها و وب‌سایت‌ها و موارد درج‌شده توسط مراجعین به آنها ۵. شناسایی و کنترل URL های مورددار ۶. جلوگیری از ورود تلفن‌های همراه دوربین‌دار و دوربین دیجیتال و حافظه‌خور به اماکن حساس

جدول ۲: راهبردهای مبتنی بر افزایش خطرهای مد نظر برای ارتکاب جرم

دسته فرعی	مصادیق
۱. تحت نظر قرار دادن ورودی ـ خروجی در اماکن عمومی	۱. استفاده از دوربین‌های مدار بسته برای کنترل ورودها و خروج‌ها ۲. استفاده از تگ‌های RFID برای شناسایی و جلوگیری از خروج غیرمجاز تجهیزات سازمانی رایانه‌ای ۳. گشت فضای مجازی ۴. در صورت امکان کنترل بسته‌های اطلاعاتی خروجی ۵. ردیابی IP ۶. نصب نرم‌افزارهای کنترل دسترسی به فضای مجازی و تهیه فایل ثبت وقایع
۲. توسعه محافظت	۱. ایمیل خود را به طور صریح در اینترنت قرار ندهید. ۲. جنسیت خود را در فضای مجازی اعلام نکنید. ۳. به سایت‌های ناشناخته و مشکوک وارد نشوید. ۴. مراقب باشید کسی متوجه رمز اینترنت یا حساب بانکی شما را نشود. ۵. فقط از رایانه خود یا رایانه مطمئن به حساب‌های بانکی خود متصل شوید. ۶. تغییر مداوم رمزها ۷. استفاده از ترکیب حرف و رقم و علایم در رمزها ۸. کوتاه نبودن و ساده نبودن رمزها (حداقل ۸ کاراکتر) ۹. باز نکردن ایمیل‌ها و لینک‌های ناشناس ۱۰. تربیت و معرفی کارشناسان تشخیص جرایم و ... مجازی
۳. تقویت نظارت رسمی	۱. کنترل و نظارت فضای مجازی ۲. استفاده از افراد متخصص امنیت شبکه برای نظارت بر سایت‌ها، وبلاگ‌ها و ... در فضای مجازی ۳. نظارت و کنترل سایت‌ها، میزبان‌ها، وبلاگ‌ها و ... و کنترل محتوا و ترافیک ورودی ـ خروجی آنها ۴. نصب دوربین در سایت‌ها ۵. وبلاگ‌ها و وب سایت‌ها، طبق قانون نسبت به موارد درج‌شده، مسئول‌اند. ۶. استفاده از ویروس‌یاب‌ها و بسته‌های امنیتی برای افزایش امنیت رایانه‌ها در برابر هک و ... ۷. در نوشتن سیاست‌های امنیتی دقت شود تا یکدیگر را نقض نکنند. ۸. تدوین قانون فضای مجازی مناسب ۹. بازدید دوره‌ای رایانه‌های متصل به اینترنت که مورد سوءاستفاده داخلی یا از راه دور قرار نگیرند. ۱۰. استفاده از رایانه‌ها منوط به وجود توکن‌های نرم‌افزاری و سخت‌افزاری شود تا در صورت سرقت آنها بدون توکن، اطلاعات و نرم‌افزارها قابل استفاده نباشد.
۴. نظارت به وسیله کارمندان	۱. در ادارات و دانشگاه و ... افرادی در سایت مستقر شوند و بر استفاده دیگران از اینترنت، نظارت کنند و همچنین تعیین مدیر برای نظارت بر سایت. ۲. در خانه، والدین بر استفاده از اینترنت فرزندان نظارت کنند. ۳. کامپیوتر متصل به اینترنت در محل عمومی قرار داده شود. ۴. مدت استفاده از اینترنت محدود شود. ۵. مدیر سایت‌ها با رصد ترافیک سایت اتصالات سوء را تشخیص دهد. ۶. استفاده خانواده‌ها از مشاورین برای بررسی استفاده درست فرزندان

دسته فرعی	مصادیق
۵. از نظارت طبیعی کمک بگیرید.	۱. قرار دادن رایانه‌های متصل به اینترنت در محل دید همگان در سایت‌های دانشگاه‌ها و ادارات تا نظارت ممکن باشد. در خانه، رایانه‌های متصل به اینترنت را در محل دید عموم قرار دهید تا نظارت ممکن باشد. در رسانه‌ها مانند صدا و سیما و در فضای مجازی مانند وب سایت‌ها و ... موارد اعمال مجازات افراد به واسطه ارتکاب جرم در فضای مجازی گزارش شود.
۶. کاهش گمنامی	۱. افراد برای استفاده از سایت‌ها، وبلاگ‌ها و ... ماهیت و تعلق سایت را شناسایی کنند. ۲. سایت‌ها ... مکلف به معرفی خود با نشان‌های استاندارد و مصوب کشور شوند و صحت ادعای آنان توسط پلیس و سایر عوامل بررسی شود. برای این کار نیاز به آرم همراه با یک شماره شناسایی منحصر به فرد است. ۳. استفاده از ابزارهای بیومتریک برای استفاده از رایانه، اینترنت و اتصال به سایت‌های حساس ۴. به کاربران در فضای مجازی یک شماره منحصر به فرد مانند کد ملی اختصاص داده شود تا گمنامی رفع شود. ۵. استفاده از وب سایت‌ها، وبلاگ‌ها و ... منوط به دریافت شناسه کاربری و رمز باشد.
۷. بهره‌گیری از ابزارهای مدیریت بر مکان	۱. استفاده از نرم‌افزارهای کنترل استفاده کودکان، نوجوانان، جوانان، دانشجویان، کارکنان و ... از اینترنت ۲. فیلتر سایت‌های مستهجن ۳. تعریف سطح دسترسی به اطلاعات سازمانی متناسب با اختیارات فرد ۴. نصب دوربین در سایت‌ها و مراکز ارائه خدمات اینترنت ۵. استفاده از ابزارهای بیومتریک برای استفاده از اینترنت و اتصال به سایت‌های حساس ۶. استفاده از نرم‌افزارهای جاسوسی (SPYWARE) برای رصد فعالیت کودکان در ساعاتی که والدین حضور ندارند.

جدول ۳: راهبردهای کاهش دستاوردهای مورد انتظار برای ارتکاب جرم یا همان سود حاصل یا کاهش منافع حاصل برای ارتکاب جرم

دسته فرعی	مصادیق
۱. زوال منافع مانند علامت‌گذاری کالا با جوهر، پاک کردن دیوارنوشته‌ها، سرعت‌گیر در خیابان	۱. فیلتر کردن سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی معاند و ضد دین و مستهجن ۲. کاهش سرعت اینترنت برای مصارف خانگی ۳. از کار انداختن سایت‌ها، وبلاگ‌ها و ... داخلی که خلاف شئونات و قوانین جامعه عمل می‌کنند. ۴. رمزنگاری نامه‌ها و فایل‌های ارسالی مهم و اطلاعات خصوصی در سایت‌ها ۵. استفاده از امضای دیجیتال و محرمانه کردن اطلاعات ۶. استفاده از برچسب‌های دیجیتالی و امضای دیجیتال روی فایل‌ها و برنامه‌های تبلیغاتی و استفاده از رمزهای غیرقابل شناسایی

دسته فرعی	مصادیق
۲. برهم‌زدن بازارهای غیرقانونی مانند نظارت بر بنگاه‌های کارگشایی، کنترل بر آگهی‌های نیازمندی‌ها، صدور مجوز برای دست‌فروشان	۱. برقراری ضابطه و قانون برای انجام تجارت الکترونیکی و موارد مرتبط در فضای مجازی ۲. برخورد با بازارهای غیرقانونی و حذف آنها ۳. نظارت بر انواع معاملات در فضای مجازی ۴. کنترل بر آگهی‌های نیازمندی‌ها در فضای مجازی ۵. صدور مجوز برای کلیه فعالیت‌ها در فضای مجازی ۶. کنترل و نظارت بر کلیه مطالب موجود در وب سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی
۳. مخفی کردن آماج، پارک نکردن خودرو در خیابان، کتابچه راهنمای تلفن بدون تعیین جنسیت	۱. درج نکردن اطلاعات کامل شخصی مانند نام کوچک در سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی ۲. درج نکردن عکس کوچک در سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی ۳. درج نکردن جنسیت در سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی ۴. عدم تبلیغ دارایی‌ها و ... در فضای مجازی ۵. درج نکردن آدرس ایمیل به طور کامل ۶. هنگام باز کردن ایمیل، کسب اطمینان از اینکه ایمیل از طرف دوست است و جعلی نیست. ۷. وب‌گردی نکردن در سایت‌ها ۸. هیچ‌گاه در مراکز عمومی مانند کافی‌نت‌ها یا مکان‌هایی که اینترنت رایگان در اختیار می‌گذارند و از امنیت آن اطمینان کافی ندارید، از ایمیل، اینترنت بانک و مواردی که برای استفاده به رمز عبور شما نیاز دارد، استفاده نکنید. ۹. اگر در مکان عمومی مجبور به استفاده از اینترنت شدید، هنگام وارد کردن رمز عبور دقت کنید که اطرافیان قادر به مشاهده رمز شما نباشند و تا جایی که ممکن است از صفحه کلید مجازی که بانک‌ها در اختیارتان می‌گذارند، استفاده کنید.
۴. از دسترس خارج کردن آماج مانند پنل پخش خودرو	
۵. جابه‌جایی و برداشتن آماج جرم مانند مثل برداشتن ضبط خودرو	۱. انتقال سرمایه‌ها و اطلاعات از اینترنت به شبکه ملی برای جلوگیری از حمله هکرهای جهانی ۲. درج نکردن اطلاعات شخصی و سازمانی روی رایانه متصل به اینترنت ۳. رمزگذاری مناسب روی رایانه، ویندوز، فایل‌ها و پوشه‌های رایانه و ایمیل و تغییر دوره‌ای آنها ۴. توجیه افراد که به ایمیل‌های ناشناس پاسخ ندهند. ۵. وارد نشدن به سایت‌ها، شبکه‌های اجتماعی و تالارهای گفت‌وگوی ناشناخته ۶. گفت‌وگوی الکترونیکی نکردن با افراد ناشناس ۷. متصل نشدن رایانه با اطلاعات شخصی/سازمانی به اینترنت

دسته فرعی	مصادیق
۶. شناسایی اموال/نشانه‌گذاری اموال مثل نشانه/علامت‌گذاری اموال و اثاثیه ذی‌قیمت، استفاده از شماره رمز برای ورود به رایانه	رمزگذاری مناسب روی رایانه، ویندوز، فایل‌ها و پوشه‌های رایانه و ایمیل و تغییر دوره‌ای آنها
۷. حذف یا کاهش جذابیت وسایل تحریک‌آمیز	۱. از بین بردن یا فیلتر کردن سایت‌های مستهجن، کلاهبرداری، دارای بی‌نزاکتی، ضد دین و ضد نظام و القاکننده افکار الحادی و آموزش خرابکاری، ساخت مواد منفجره، آموزش هک و ... ۲. افراد دارای وب سایت، وبلاگ و ... از قید نام کوچک خودداری کنند و عکس و اطلاعات شخصی و خصوصی خود را در سایت یا وبلاگ و ... قرار ندهند. ۳. قرار ندادن صریح آدرس ایمیل خود در سایت، وبلاگ و ... برای جلوگیری از حمله توسط برنامه‌ها و ... ۴. افراد دارایی‌ها و امکانات مادی خود را در فضای مجازی معرفی نکنند تا کمتر در معرض خطر قرار گیرند. ۵. ایجاد سایت فرهنگی، علمی و هنری منطبق با فرهنگ اسلامی و تبیین زندگی چهارده معصوم(ع) و انسان متعالی از دیدگاه قرآن و اسلام ۶. فرهنگ‌سازی استفاده درست از اینترنت ۷. آگاه‌سازی متناسب با سن افراد مختلف به شیوه‌های مختلف مانند سخنرانی، مصاحبه، کلیپ، فیلم درباره آسیب‌های فضای مجازی ۸. اطلاع‌رسانی عواقب ناشی از ارتکاب جرم در فضای مجازی به شیوه‌های مختلف مانند سخنرانی، مصاحبه، کلیپ، فیلم ۹. آگاه‌سازی تبعات ناشی از ورود به سایت‌های مستهجن و مسئله‌دار و ارتباط با افراد ناشناس
۸. تضییق یا جلوگیری از منافع	۱. آگاه‌سازی کاربران اینترنت از آسیب‌ها ۲. رمزگذاری مناسب روی رایانه، ویندوز، فایل‌ها و پوشه‌های رایانه و ایمیل و تغییر دوره‌ای آنها ۳. درج کردن عکس و اطلاعات کامل شخصی در فضای مجازی ۴. رمزدار کردن اطلاعات ارسالی در فضای مجازی

جدول ۴: راهبرد حذف توجیه‌کننده‌ها یا عوامل تحریک یا تشویق فرد به ارتکاب جرم

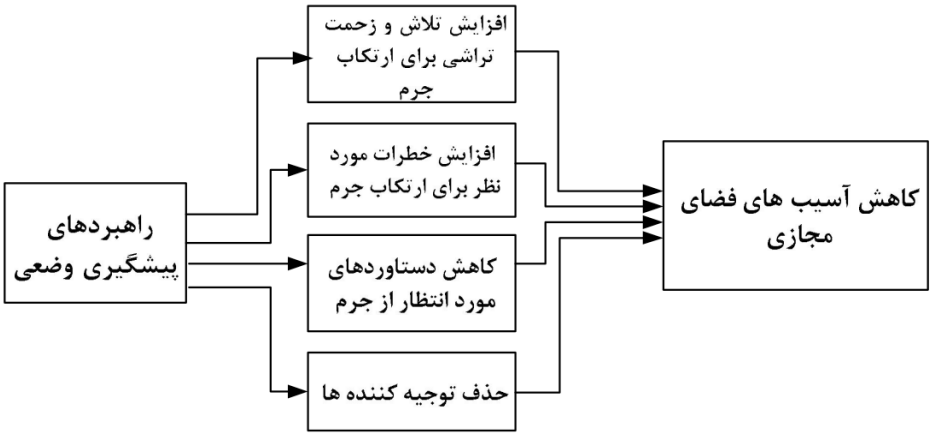
دسته فرعی	مصادیق
۱. برقراری/ وضع قواعد/ مقررات مانند قراردادهای اجاره، وضع مقررات برای مزاحمت	۱. وضع مقررات برای انجام هر گونه فعالیت در فضای مجازی به نحوی که انجام هر فعالیت منوط به اخذ مجوز از مراجع ذی‌صلاح شود. ۲. وضع مقررات برای ایجاد وب سایت، وبلاگ، شبکه اجتماعی مجازی و ... ۳. تدوین قانون جرایم سایبری برای انواع ارتکاب جرم در فضای مجازی و اطلاع‌رسانی آن از طریق رسانه‌ها شامل صدا و سیما، وب سایت‌ها، وبلاگ‌ها و ... به نحوی که کسی نتواند ادعا کند به دلیل عدم آگاهی مرتکب تخلف در فضای مجازی شده است. ۴. در سایت‌های اینترنت دانشگاهی، اداری و دانش‌آموزی اطلاع‌رسانی شود که ایجاد ارتکاب جرم، کلاهبرداری، ارتکاب جرم از طریق ارسال ایمیل، ایجاد وب سایت، تالار گفت‌وگو و ... ضمن لغو مجوز استفاده از اینترنت، برابر قانون مستوجب مجازات است. ۵. تبیین مصادیق ارتکاب جرم در فضای مجازی و رسانه‌ها
۲. پست راهنما برای مثال پارک نکنید، ملک خصوصی است.	۱. درج راهنما در سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی به شیوه‌های مختلف مانند کلیپ، فیلم و... ۲. مصادیق ارتکاب جرم در فضای مجازی و رسانه‌ها ۳. انواع آسیب‌های فضای مجازی ۴. نحوه مراقبت از خود در برابر آسیب‌های فضای مجازی ۵. استفاده از پهنای باند اینترنت دیگران جرم است. ۶. ارتکاب جرم در همه جا از جمله فضای مجازی جرم است. ۷. نقض حریم خصوصی در همه جا از جمله فضای مجازی جرم است. ۸. درج موارد خلاف شئونات و ... در سایت‌ها، وبلاگ‌ها، شبکه‌های اجتماعی و ... جرم است.
۳. تحریک/ هوشیاری وجدان و آگاهی	۱. مصادیق آسیب در فضای مجازی نیز صادق است. ۲. رعایت حق نشر در فضای مجازی مانند فضای فیزیکی ضروری است. ۳. اطلاع‌رسانی موارد ذیل در وب سایت‌ها، وبلاگ‌ها و ... به شیوه‌های مختلف مانند کلیپ، فیلم و... ۴. همان‌گونه که در فضای فیزیکی باید متدین بود، باید در فضای مجازی هم متدین بود. ۵. ارائه تصویر غیر واقعی از خود در فضای مجازی مظهر دروغگویی و کلاهبرداری است. ۶. در همه جا باید صادق بود. ۷. ارتکاب جرم در فضای مجازی مانند دنیای فیزیکی جرم است. ۸. آگاه‌سازی همگان از آسیب‌های فضای مجازی به شیوه‌های مختلف مانند کلیپ، فیلم و... برای محافظت از خود در فضای مجازی ۹. اطلاع‌رسانی مجازات‌های تعیین‌شده برای انواع ارتکاب جرم و آسیب‌رسانی در فضای مجازی ۱۰. اطلاع‌رسانی آسیب‌رسانان دستگیرشده ۱۱. هوشیار کردن مردم از طریق رسانه‌ها درباره جرایم و پیشگیری از جرایم در محیط خانواده‌ها با بالا بردن سطح هوشیاری و دانش خانواده که بعضاً با فضای مجازی بیگانه هستند.

دسته فرعی	مصادیق
۴. تسهیل رعایت قوانین	۱. ایجاد مرکز مشاع استفاده از اینترنت در محیط‌های سازمانی ۲. تشویق و ایجاد انگیزه در استفاده مجاز از فضای مجازی ۳. ایجاد محیط‌های ورزشی و فرهنگی و ترغیب به استفاده از آنها به جای استفاده از اینترنت ۴. ایجاد سایت‌ها وشبکه‌های آموزشی و فرهنگی و علمی مجاز
۵. کنترل مواد مخدر	۱. کنترل نرم‌افزاری اتصال فرزندان به سایت‌ها، وبلاگ‌ها و ... ۲. بررسی ویروسی نشدن رایانه فرزندان براثر استفاده از اینترنت ۳. بررسی ویروسی نشدن رایانه دانشجویان براثر استفاده از اینترنت ۴. کنترل رفتار فرزندان که دچار اعتیاد اینترنتی یا اعتیاد به بازی‌های رایانه‌ای نشده باشند. ۵. کنترل رفتار فرزندان که مرتکب ارتکاب جرم در فضای مجازی نشوند. ۶. استفاده از نرم‌افزارهای کنترل اتصال دانشجویان/کارکنان به سایت‌های مختلف ۷. کنترل سایت‌ها، وبلاگ‌ها و ... توسط پلیس فتا
۶. کنترل رهاکننده‌ها مانند نصب تراشه‌های مخصوص روی تلویزیون و رایانه برای استفاده کنترل‌شده از آنها	۱. نصب نرم‌افزارهای کنترل‌کننده اتصال به سایت‌ها، وبلاگ‌ها و موارد مسئله‌دار ۲. عدم اعطای کاربری مدیر به فرزندان در خانه برای جلوگیری از نصب فیلترشکن ۳. عدم اعطا کاربری مدیر به دانشجویان در دانشگاه برای جلوگیری از نصب فیلترشکن ۴. کنترل ویندوز رایانه متصل به اینترنت که فایل یا پوشه‌ای در آن به اشتراک گذاشته نشده باشد. ۵. کنترل ویندوز رایانه متصل به اینترنت که گزینه دسترسی از راه دور فعال نشده باشد. ۶. طراحی نرم‌افزاری کنترل‌کننده اطلاعات یا نمایش‌دهنده سرقت اطلاعات از سیستم‌های اطلاعاتی مهم

۶. چارچوب نظری تحقیق

براساس راهبردهای ارائه‌شده، برای پیشگیری وضعی از آسیب‌های فضای مجازی، مدل مفهومی راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی مطابق شکل ۱ است. مطابق این مدل مفهومی، راهبردهای پیشگیری وضعی به چهار دسته زیر تقسیم می‌شوند:

۱. افزایش تلاش و زحمت برای ارتکاب جرم
۲. افزایش خطرهای مد نظر برای ارتکاب جرم
۳. کاهش دستاوردهای مورد انتظار از برای ارتکاب جرم
۴. حذف توجیه‌کننده‌ها



شکل ۱: مدل مفهومی راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی

۷. نوع و روش تحقیق

تحقیق حاضر از نظر هدف، به دنبال استفاده از راهبردهای پیشگیری وضعی برای جلوگیری از آسیب‌های فضای مجازی است؛ از این رو از نوع کاربردی است و چون نظر کارشناسان درباره راهبردهای پیشگیری وضعی ارائه‌شده برای پیشگیری از آسیب‌های فضای مجازی اخذ می‌شود، از نظر ماهیت از نوع پیمایشی است. در انجام این تحقیق از شیوه کتابخانه‌ای شامل مطالعات داخلی و خارجی و میدانی استفاده شده است. جامعه آماری تحقیق کارشناسان رشته‌های تحصیلی کامپیوتر، فناوری اطلاعات، علوم کامپیوتر و مخابرات در شهر تهران هستند که تعدادشان بالغ بر ۱۰۰۰۰۰ نفر است و با توجه به حجم جامعه، حجم نمونه براساس جدول مرگان، ۳۸۴ نفر در نظر گرفته شده است. نمونه‌گیری به صورت ترکیبی (گلوله برفی و تصادفی) انجام شده است. برای جمع‌آوری اطلاعات از پرسشنامه پنج‌گزینه‌ای استفاده شد. با توجه به راهبردهای ارائه‌شده برای پیشگیری از آسیب‌های فضای مجازی بر مبنای راهبردهای پیشگیری وضعی ارائه‌شده، پرسشنامه‌ای برای اخذ نظر کارشناسان و خبرگان درباره راهبردهای پیشنهادی طراحی و پاسخ کاربران بر مبنای طیف لیکرت دریافت شد. پرسشنامه شامل ۴۹ سؤال است که در چهار بخش طراحی شده است. زمان اجرای تحقیق سال ۱۳۹۲ است.

برای افزایش روایی پرسشنامه از پیش‌آزمون استفاده شد. ابتدا پرسشنامه میان ۲۰ تن از خبرگان جامعه آماری توزیع و دیدگاه اصلاحی آنان در پرسشنامه اعمال و پس از آن پرسشنامه نهایی توزیع شد. برای آزمون پایایی پرسشنامه از روش محاسبه آلفای کرونباخ استفاده شده است؛ بدین ترتیب که پس از طراحی ابزار اندازه‌گیری، ابتدا آزمون مقدماتی صورت گرفت و پرسشنامه میان ۲۰ تن از افراد جامعه آماری توزیع و جمع‌آوری شد و مقدار آلفای کرونباخ پرسشنامه با استفاده از نرم‌افزار SPSS ۰/۹۵ به دست آمد؛ بنابراین پرسشنامه طراحی‌شده از اعتبار کافی برای ارزیابی نقش و شاخص‌ها برخوردار است. برای بررسی میزان اعتبار و پایایی این تحقیق از نرم‌افزار SPSS استفاده شد و مقدار آلفای کرونباخ پرسشنامه ۹۷/. به دست آمد. این عدد برای یک پرسشنامه محقق‌ساخته عدد مطلوب و قابل قبولی است و نشان می‌دهد پرسش‌های طرح‌شده از اعتبار کافی برای ارزیابی شاخص‌ها برخوردار است.

۸. تجزیه و تحلیل راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی

سؤال: چه راهبردهایی برای پیشگیری وضعی از آسیب‌های فضای مجازی وجود دارد؟

اطلاعات جدول ۵ نشان می‌دهد که نمونه مورد بررسی «تأثیر راهبردهای مبتنی بر افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم تأثیر زیادی در پیشگیری از آسیب‌های فضای مجازی دارد»، که با توجه به T محاسبه‌شده و سطح معنی‌داری به‌دست‌آمده (Sig =۰/۰۰۰)، می‌توان گفت تأثیرگذاری برحسب نظر نمونه مورد بررسی معنادار است.

جدول ۵: نتایج آزمون T تک نمونه برای بررسی راهبردهای مبتنی بر افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم

فراوانی	میانگین	انحراف استاندارد	تفاوت میانگین	DF	T	Sig
۳۷۰	۶۱/۳	۵۹/۰	۶۱/۰	۳۶۹	۲۰	۰۰۰/۰

اطلاعات جدول ۶ نشان می‌دهد برحسب نظر نمونه مورد بررسی، تأثیر راهبردهای مبتنی بر افزایش خطرهای مد نظر برای ارتکاب جرم در پیشگیری از آسیب های فضای مجازی زیاد است که با توجه به T محاسبه‌شده و سطح معنی‌داری (Sig =۰/۰۰۰) به‌دست‌آمده، این تأثیر معنادار است.

جدول ۶: نتایج آزمون T تک نمونه برای بررسی تأثیر راهبردهای مبتنی بر افزایش خطرهای مد نظر برای ارتکاب جرم

فراوانی	میانگین	انحراف استاندارد	تفاوت میانگین	DF	T	Sig
۳۷۰	۵۸/۳	۶۸/۰	۵۸/۰	۳۶۹	۳۱/۱۶	۰۰۰/۰

اطلاعات جدول ۷ نشان می‌دهد برحسب نظر نمونه مورد بررسی، تأثیر کاهش دستاوردهای مورد انتظار از ارتکاب جرم یا همان سود حاصل یا کاهش منافع حاصل از جرم در پیشگیری از آسیب‌های فضای مجازی زیاد است که با توجه به T محاسبه‌شده و سطح معنی‌داری (Sig =۰/۰۰۰) به‌دست‌آمده، این تأثیر معنادار است.

جدول ۷: نتایج آزمون T تک نمونه برای بررسی تأثیر کاهش دستاوردهای مورد انتظار از ارتکاب جرم در پیشگیری از مسائل فضای مجازی

فراوانی	میانگین	انحراف استاندارد	تفاوت میانگین	DF	T	Sig
۳۷۰	۶۴/۳	۶۸/۰	۶۸/۰	۳۶۹	۸۹/۱۷	۰۰۰/۰

اطلاعات جدول ۸ نشان می‌دهد برحسب نظر نمونه مورد بررسی، تأثیر حذف توجیه‌کننده‌ها یا از بین بردن عوامل تحریک یا تشویق فرد به ارتکاب جرم در پیشگیری از آسیب‌های فضای مجازی زیاد است که با توجه به T محاسبه‌شده و سطح معنی‌داری (Sig =۰/۰۰۰) به‌دست‌آمده، این تأثیر معنادار است.

جدول ۸: نتایج آزمون T تک نمونه برای بررسی تأثیر حذف توجیه‌کننده‌ها به ارتکاب جرم در پیشگیری از مسائل فضای مجازی

فراوانی	میانگین	انحراف استاندارد	تفاوت میانگین	DF	T	Sig
۳۷۰	۶۹/۳	۶۸/۰	۶۹/۰	۳۶۹	۴۸/۱۹	۰۰۰/۰

اطلاعات مندرج در جدول‌های ۹ و ۱۰ میانگین رتبه‌ای هر یک از ابعاد پیشگیری وضعی در جلوگیری از آسیب‌های فضای مجازی را نشان می‌دهد؛ به طوری که می‌توان گفت حذف توجیه‌کننده‌ها، کاهش منافع حاصل از جرم، افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم و افزایش خطرهای مد نظر برای ارتکاب جرم به ترتیب بالاترین تا پایین‌ترین میانگین

رتبه‌ای را به خود اختصاص داده‌اند که با توجه به نتایج آزمون کای اسکویر، این تفاوت‌ها معنی‌دار است.

جدول ۹: نتایج آزمون رتبه‌بندی فریدمن برای ابعاد پیشگیری وضعی

ردیف	ابعاد پیشگیری وضعی	میانگین
۱	حذف توجیه‌کننده‌ها به ارتکاب جرم	۷۸/۲
۲	کاهش منافع حاصل از جرم	۵۱/۲
۳	افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم	۴۰/۲
۴	افزایش خطرهای مد نظر برای ارتکاب جرم	۳۱/۲

جدول ۱۰، نتایج آزمون کای اسکویر برای بررسی تفاوت میانگین‌های رتبه‌ای را نشان می‌دهد.

جدول ۱۰: نتایج آزمون کای اسکویر برای بررسی تفاوت میانگین‌های رتبه‌ای

N	chi-square	dF	Sig
۳۷۰	۴۹/۲۷	۳	۰۰۰/۰

میانگین سؤال‌های پرسشنامه پیشگیری وضعی از آسیب‌ها و ...: جدول ۱۱ میانگین گویه‌های مربوط به راهبردهای مبتنی بر افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم در پیشگیری وضعی از آسیب‌های فضای مجازی را نشان می‌دهد. مطابق مندرجات این جدول، کل گویه‌ها میانگین محاسبه‌شده بالاتر از حد متوسط (۳) دارند. دیگر اینکه از نظر پاسخ‌دهندگان، گویه‌های ۱. نصب ویروس‌یاب و به‌روز نگه داشتن آن روی رایانه، نصب دیواره آتش ویندوز و ...؛ ۲. رمزگذاری روی فایل‌ها، پوشه‌ها، رایانه، ویندوز، برپاسازی[1] ویندوز و تغییر منظم آنها و ... و ۳. ایجاد سایت‌ها، شبکه‌های اجتماعی مجازی و ... در زمینه امور آموزشی، فرهنگی، هنری، علمی و ... دارای بالاترین میانگین و گویه‌های ۱. جمع‌آوری مراکز فروش رسانه‌های رایانه‌ای غیرمجاز و ...؛ ۲. محدود کردن زمان استفاده از اینترنت برای کودکان، نوجوانان و ... و ۳. ارائه کلیه خدمات الکترونیکی (عابر بانک) و اینترنتی به

1. SETUP

افراد بر مبنای تأیید مراجع ذی‌صلاح و ... در زمینه امور آموزشی، فرهنگی، هنری، علمی و... پایین‌ترین میانگین را دارند.

جدول ۱۱: میانگین گویه‌های مربوط به راهبردهای مبتنی بر افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم

گویه‌های سخت کردن آماج جرم	نمره
نصب ویروس‌یاب و به‌روز نگه‌داشتن آن روی رایانه، نصب دیواره آتش ویندوز و ورودی شبکه و عدم ذخیره رمز عبور در نرم‌افزارهای مرورگر وب	۱۰/۴
خارج کردن درایوهای ویندوز از حالت اشتراکی پیش‌فرض و از دسترس خارج کردن از راه دور کامپیوترها (Remote....)	۶۷/۳
رمزگذاری روی فایل‌ها، پوشه‌ها، رایانه، ویندوز، SETUP ویندوز و تغییر منظم آنها و استفاده نکردن از مشخصات شخصی مثل سال تولد، شماره شناسنامه، رمزهای پیش‌فرض برای رمز و یکسان نبودن عنوان شناسه کاربری و رمز و استفاده از ترکیب حرف و رقم برای رمز	۷۱/۳
گویه‌های کنترل ورودی‌ها به اماکن مختلف یا کنترل دسترسی به اماکن، تجهیزات و اهداف مربوط	
استفاده از اینترنت با دریافت شناسه کاربری و رمز و نظارت و کنترل استفاده با نرم‌افزارهای کنترل ترافیک شبکه و ثبت وقایع برای بررسی سوءاستفاده، ارتکاب جرم و ... کاربران و در صورت لزوم لغو مجوز استفاده آنان	۶۶/۳
ارائه تمام خدمات الکترونیکی (عابر بانک) و اینترنتی به افراد بر مبنای تأیید مراجع ذی‌صلاح و کسب صلاحیت لازم	۴۶/۳
پرهیز در دانلود، اجرا و استفاده از نرم‌افزارهای ناشناخته و نامطمئن برای امور مختلف مانند اتصال به اینترنت و باز نکردن ایمیل‌های ناشناخته و مشکوک	۶۶/۳
گویه‌های کنترل خروجی‌ها	
استفاده از تگ‌های RFID برای شناسایی و جلوگیری از خروج غیرمجاز تجهیزات سازمانی	۶۸/۳
استفاده از دوربین‌های مدار بسته برای کنترل ورودها و خروج‌ها	۴۸/۳
گویه‌های تغییر برای اعمال مجرمانه مرتکبان یا منحرف کردن بزهکاران از آماج	
محدود کردن زمان استفاده از اینترنت برای کودکان، نوجوانان و تنظیم برنامه‌های مفرح برای آنان	۴۴/۳
ایجاد سایت‌ها، شبکه‌های اجتماعی مجازی و ... در زمینه امور آموزشی، فرهنگی، هنری، علمی و ... منطبق با فرهنگ اسلامی و متناسب با سن افراد از جمله ایجاد و ترویج بازی‌های رایانه‌ای منطبق با فرهنگ اسلامی	۷۰/۳
نمایش عواقب ارتکاب جرم و ... در فضای مجازی از طریق روش‌های مختلف مانند صدا، سیما، در سایت‌ها و ...	۶۶/۳

گویه‌های کنترل و ایجاد محدودیت برای استفاده از ابزارهای تسهیل ارتکاب جرم یا کنترل ابزار جرم/سلاح‌ها	
جمع‌آوری مراکز فروش رسانه‌های رایانه‌ای غیرمجاز، فیلترشکن‌ها از سایت‌ها یا فیلتر کردن سایت‌های مسئله‌دار	۳۵/۳
ندادن شناسه کاربری مدیر به کاربران برای نصب نرم‌افزارهای سازمانی یا فیلترشکن روی رایانه‌های متصل به اینترنت	۵۵/۳
گویه‌های کنترل ابزارآلات جرم/سلاح‌ها	
ایجاد یک رویه برای تعیین صلاحیت وب سایت‌ها، وبلاگ‌ها و ... توسط مراجع ذی‌صلاح و درج نمادی در وبلاگ، وب سایت و .... که نشان‌دهنده واجد شرایط بودن آنهاست.	۵۸/۳
انجام گشت سایبری در فضای مجازی و شناسایی سایت‌های دارای فیلترشکن و موارد مسئله‌دار و شناسایی و کنترل URL های موردار و برخورد قانونی با آنها	۵۱/۳

جدول ۱۲ میانگین گویه‌های مربوط به راهبردهای افزایش خطرهای مد نظر برای ارتکاب جرم در پیشگیری وضعی از آسیب‌های فضای مجازی را نشان می‌دهد. مطابق مندرجات این جدول، کل گویه‌ها میانگین محاسبه‌شده بالاتر از حد متوسط (۳) دارند. دیگر اینکه از نظر پاسخ‌دهندگان، گویه‌های ۱. ردیابی IP ارسال‌کنندگان هرزنامه و موارد مسئله‌دار؛ ۲. نظارت والدین بر استفاده فرزندان از اینترنت و ۳. اتصال به حساب‌های بانکی شخصی از طریق رایانه خود یا رایانه مطمئن دارای بالاترین میانگین و گویه‌های ۱. کامپیوترهای متصل به اینترنت در محل عمومی قرار داده شود تا نظارت ممکن باشد؛ ۲. استفاده از نرم‌افزارهای کنترل استفاده کاربران، فرزندان و ... و ۳. بازدید دوره‌ای رایانه‌های متصل به اینترنت که مورد سوءاستفاده داخلی یا از راه دور قرار نگرفته باشند، پایین‌ترین میانگین را دارند.

جدول ۱۲: میانگین گویه‌های مربوط به افزایش خطرهای مد نظر برای ارتکاب جرم

گویه‌های تحت نظر قرار دادن ورودی- خروجی در اماکن عمومی	نمره
ردیابی IP ارسال‌کنندگان هرزنامه و موارد مسئله‌دار	۸۱/۳
گویه‌های توسعه محافظت	
درج نکردن صریح آدرس ایمیل و اطلاعات شخصی مانند اسم کوچک، جنسیت، سن، وضع مالی، محل سکونت و ... در کلوپ‌ها و سایت‌ها و شبکه‌های اجتماعی و رایانه متصل به اینترنت	۵۹/۳
اتصال به حساب‌های بانکی شخصی از طریق رایانه خود یا رایانه مطمئن	۷۳/۳

گویه‌های تقویت نظارت رسمی	
کنترل و نظارت بر سایت‌ها، وبلاگ‌ها، میزبان‌ها و ... از طریق مراجعه و کنترل محتوا و ترافیک ورودی ـ خروجی آنها با استفاده از افراد متخصص فناوری اطلاعات و امنیت شبکه توسط سازمان‌های ذی‌ربط و پلیس فتا	۶۴/۳
بازدید دوره‌ای رایانه‌های متصل به اینترنت که مورد سوءاستفاده داخلی یا از راه دور قرار نگرفته باشند.	۴۶/۳
گویه‌های نظارت به وسیله کارمندان	
تعیین مسئول سایت برای نظارت بر استفاده کاربران از اینترنت و رصد ترافیک سایت برای تشخیص اتصالات سوء	۵۵/۳
نظارت والدین بر استفاده فرزندان از اینترنت	۷۳/۳
گویه‌های از نظارت طبیعی کمک بگیرید.	
کامپیوترهای متصل به اینترنت در محل عمومی قرار داده شود تا نظارت ممکن باشد.	۳۶/۳
گویه‌های کاهش گمنامی	
سایت‌ها، وبلاگ و ... مکلف به معرفی خود با نشان‌های مصوب شوند و صحت ادعای آنان توسط پلیس و سایر مراجع ذی‌صلاح بررسی شود و در صورت مجاز بودن توسط کاربران استفاده شوند.	۵۵/۳
استفاده از وب‌سایت‌ها، وبلاگ‌ها و ... منوط به دریافت شناسه کاربری و رمز یا ابزارهای بیومتریک	۳۸/۳
گویه‌های بهره‌گیری از ابزارهای مدیریت بر مکان	
استفاده از نرم‌افزارهای کنترل استفاده کاربران، فرزندان و ... به سایت‌ها، وبلاگ‌ها و ... مسئله‌دار	۵۵/۳

جدول ۱۳ میانگین گویه‌های مربوط به راهبردهای کاهش دستاوردهای مورد انتظار از ارتکاب جرم یا همان سود حاصل یا کاهش منافع حاصل از جرم در پیشگیری وضعی از آسیب‌های فضای مجازی را نشان می‌دهد. مطابق مندرجات این جدول، کل گویه‌ها میانگین محاسبه‌شده بالاتر از حد متوسط (۳) دارند. دیگر اینکه از نظر پاسخ‌دهندگان، گویه‌های ۱. دقت در وارد کردن رمز عبور هنگام استفاده از اینترنت... و ۲. برقراری ضابطه و قانون برای انجام همه فعالیت‌ها در فضای مجازی مانند تجارت الکترونیکی دارای بالاترین میانگین و گویه‌های ۱. کنترل و نظارت بر کلیه مطالب موجود در وب سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی و ۲. استفاده نکردن از پست الکترونیک، اینترنت بانک و مواردی که برای استفاده به رمز عبور شما نیاز دارد از طریق اینترنت... پایین‌ترین میانگین هستند.

جدول ۱۳: میانگین گویه‌های مربوط به راهبردهای کاهش دستاوردهای مورد انتظار از ارتکاب جرم یا کاهش منافع حاصل از جرم

گویه‌های زوال منافع مانند علامت‌گذاری کالا با جوهر، پاک کردن دیوارنوشته‌ها، سرعت‌گیر در خیابان	میانگین
فیلتر کردن/ از کار انداختن سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی خلاف شئونات و قوانین جامعه، معاند و ضد دین و مستهجن و سایت‌ها	۷۲/۳
استفاده از برچسب‌های دیجیتالی و امضای دیجیتال روی فایل‌ها و برنامه‌های تبلیغاتی و استفاده از رمزهای غیر قابل شناسایی	۵۸/۳
گویه‌های برهم‌زدن بازارهای غیرقانونی مانند نظارت بر بنگاه‌های کارگشایی، کنترل آگهی‌های نیازمندی‌ها	
برقراری ضابطه و قانون برای انجام همه فعالیت‌ها در فضای مجازی مانند تجارت الکترونیکی	۷۹/۳
نظارت بر انواع معاملات و آگهی‌های نیازمندی‌ها در فضای مجازی و برخورد با بازارهای غیرقانونی و حذف آنها در فضای مجازی	۶۷/۳
کنترل و نظارت بر همه مطالب موجود در وب سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی	۳۸/۳
گویه‌های مخفی کردن آماج، پارک نکردن خودرو در خیابان، کتابچه راهنمای تلفن بدون تعیین جنسیت	
استفاده نکردن از ایمیل، اینترنت بانک و مواردی که برای استفاده به رمز عبور شما نیاز دارد از طریق اینترنت مراکز عمومی مانند کافی نت‌ها یا مکان‌های با اینترنت رایگان که از امنیت آن اطمینان کافی ندارید.	۴۲/۳
دقت در وارد کردن رمز عبور هنگام استفاده از اینترنت در مکان عمومی یا عابر بانک تا دیگران قادر به مشاهده رمز شما نباشند و در حد ممکن استفاده از صفحه کلید مجازی بانک‌ها	۸/۳
گویه‌های از دسترس خارج کردن آماج مانند پنل پخش خودرو، استفاده از کارت اعتباری برای تلفن عمومی	
اتصال شبکه‌های سازمان‌های دولتی و خصوصی مورد استفاده داخل کشور به شبکه ملی کشور مانند اطلاعات بانک‌ها	**۵۹/۳**
گویه‌های جابه‌جایی و برداشتن آماج جرم مثل برداشتن ضبط خودرو، حذف کنتورهای سکه‌ای گاز و امثال آن از خانه‌ها	
اتصال شبکه‌های سازمان‌های دولتی و خصوصی مورد استفاده داخل کشور به شبکه ملی کشور مانند اطلاعات بانک‌ها	۶۰/۳
گویه‌های حذف یا کاهش جذابیت وسایل تحریک‌آمیز	
اطلاع‌رسانی عواقب ناشی از ارتکاب جرم در فضای مجازی و تبعات ناشی از ورود به سایت‌های مستهجن و مسئله‌دار و ارتباط با افراد ناشناس به شیوه‌های مختلف مانند سخنرانی، مصاحبه، کلیپ، فیلم	۷۴/۳
ایجاد سایت فرهنگی، علمی و هنری برای فرهنگ‌سازی و آگاه‌سازی متناسب با سن افراد به شیوه‌های مختلف مانند سخنرانی، مصاحبه و کلیپ در مورد استفاده درست از اینترنت و آسیب‌های فضای مجازی	۷۴/۳

جدول ۱۴ میانگین گویه‌های مربوط به راهبردهای حذف توجیه‌کننده‌ها یا از بین بردن عوامل تحریک یا تشویق فرد به ارتکاب جرم در پیشگیری وضعی از آسیب‌های فضای مجازی را نشان می‌دهد. مطابق مندرجات این جدول، کل گویه‌ها میانگین محاسبه‌شده بالاتر از حد متوسط (۳) دارند. دیگر اینکه از نظر پاسخ‌دهندگان، گویه‌های ۱. کنترل رفتار فرزندان از نظر ابتلا به اعتیاد اینترنتی یا بازی‌های رایانه‌ای...؛ ۲. تدوین قانون جرایم سایبری برای انواع ارتکاب جرم ... و ۳. بررسی ویروسی نشدن رایانه کاربران و فرزندان براثر استفاده نامناسب یا ناآگاهانه از اینترنت دارای بالاترین میانگین و گویه‌های ۱. وضع مقررات برای انجام هر گونه فعالیت اقتصادی، اجتماعی و ایجاد وب سایت، وبلاگ، شبکه اجتماعی مجازی و ...در فضای مجازی ...؛ ۲. نصب نرم‌افزارهای کنترل‌کننده و محدودکننده اتصال به سایت‌ها، وبلاگ‌ها و موارد مسئله‌دار... و ۳. تبیین نحوه مراقبت از خود در برابر آسیب‌های فضای مجازی پایین‌ترین میانگین را دارند.

جدول ۱۴: میانگین گویه‌های مربوط به راهبردهای حذف توجیه‌کننده‌ها یا از بین بردن عوامل تحریک یا تشویق فرد به ارتکاب جرم

گویه‌های برقراری/وضع قواعد/ مقررات مانند قراردادهای اجاره و وضع مقررات برای مزاحمت	نمره
وضع مقررات برای انجام هر گونه فعالیت اقتصادی، اجتماعی و ایجاد وب سایت، وبلاگ، شبکه اجتماعی مجازی و ... در فضای مجازی به نحوی که انجام هر فعالیت منوط به اخذ مجوز از مراجع ذی‌صلاح شود.	۵۱/۳
تدوین قانون جرایم سایبری برای انواع ارتکاب جرم در فضای مجازی و اطلاع‌رسانی آن از طریق رسانه‌ها شامل صدا و سیما، وب‌سایت‌ها، وبلاگ‌ها و ... به نحوی که کسی نتواند ادعا کند به دلیل آگاهی نداشتن مرتکب تخلف در فضای مجازی شده است.	۸۸/۳
گویه‌های پست راهنما مانند پارک نکنید یا ملک خصوصی است.	
درج راهنما در سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی به شیوه‌های مختلف مانند کلیپ، فیلم و... در مورد مصادیق ارتکاب جرم مجازی مانند «استفاده از پهنای باند اینترنت دیگران جرم است»، «نقض حریم خصوصی در همه جا از جمله فضای مجازی جرم است».	۶۹/۳
اطلاع‌رسانی در فضای مجازی که ارتکاب جرم از طریق ارسال ایمیل، ایجاد وب سایت، تالار گفت‌وگو و ...، ضمن لغو مجوز استفاده از اینترنت، برابر قانون مستوجب مجازات است.	۶۶/۳
تبیین نحوه مراقبت از خود در برابر آسیب‌های فضای مجازی و مصادیق ارتکاب جرم در فضای مجازی و رسانه‌ها	۶۳/۳

گویه‌های تحریک/هوشیاری وجدان و آگاهی	
اطلاع‌رسانی آسیب‌رسانان دستگیرشده و مجازات‌های تعیین‌شده برای انواع ارتکاب جرم در فضای مجازی	۷۳/۳
اطلاع‌رسانی مواردی مانند اینکه «در فضای مجازی هم باید متدین بود»، «ارائه تصویر غیر واقعی از خود در فضای مجازی مظهر دروغ‌گویی و کلاهبرداری است»، «ارتکاب جرم در فضای مجازی جرم است» از طریق وب سایت‌ها، وبلاگ‌ها و ... به شیوه‌های مختلف مانند کلیپ، فیلم و...	۶۴/۳
اطلاع‌رسانی آسیب‌های فضای مجازی به شیوه‌های مختلف مانند کلیپ، فیلم و...در فضای مجازی و رسانه‌ها	۶۷/۳
گویه‌های کنترل مواد مخدر	
بررسی ویروسی نشدن رایانه کاربران، فرزندان براثر استفاده نامناسب یا ناآگاهانه از اینترنت	۷۷/۳
کنترل رفتار فرزندان از نظر ابتلا به اعتیاد اینترنتی یا بازی‌های رایانه‌ای، یا انجام ارتکاب جرم در فضای مجازی	۹۱/۳
کنترل مداوم حساب‌های بانکی و کسب اطمینان از تغییر موجودی، رمز	۶۵/۳
گویه‌های کنترل رهاکننده‌ها مانند نصب تراشه مخصوص روی رایانه برای استفاده کنترل‌شده از آنها یا جلوگیری از دسترسی به برنامه‌ها	
نصب نرم‌افزارهای کنترل‌کننده و محدودکننده اتصال به سایت‌ها، وبلاگ‌ها و موارد مسئله‌دار	۵۸/۳

نتیجه‌گیری

در این تحقیق مشاهده شد گسترش فناوری اطلاعات و ارتباطات و افزایش استفاده از فضای مجازی برای انجام امور مختلف سازمانی و شخصی، ضمن مزایای فراوانی که برای جامعه به ارمغان می‌آورد، به دلیل ویژگی‌های خاص این فضا، سبب گسترش سریع انواع آسیب‌ها و جرایم می‌شود؛ از این رو اتخاذ تدابیر برای پیشگیری از آسیب‌های فضای مجازی امری ضروری و اجتناب‌ناپذیر است و غفلت از این امر مهم، صدمات جبران‌ناپذیر متنوع و گسترده‌ای در ابعاد مختلف بر جامعه وارد می‌سازد. یکی از رویکردهای پیشگیری از جرم، پیشگیری وضعی است که راهبردهایی را در قالب پنج دسته برای پیشگیری از جرم ارائه می‌دهد. در این تحقیق با بهره‌گیری از این رویکرد پیشگیری و مطالعات کتابخانه‌ای انجام‌شده و تجارب محقق در حوزه فناوری اطلاعات، مدل مفهومی پیشگیری وضعی از آسیب‌های فضای مجازی استخراج و راهبردهایی برای پیشگیری از آسیب‌های فضای مجازی ارائه شد و برای اعتبارسنجی و تعیین میزان تأثیر هریک از راهبردها در پیشگیری

از آسیب‌های فضای مجازی از نظر جامعه کارشناسان مرتبط، پرسشنامه محقق‌ساخته‌ای طراحی و میان جامعه آماری تحقیق توزیع و جمع‌آوری شد و مورد تجزیه و تحلیل قرار گرفت. نتایج نشان داد:

ـ در زمینه راهبردهای پیشگیری وضعی از مسائل فضای مجازی، ابعاد حذف توجیه‌کننده‌ها، کاهش منافع حاصل از جرم، افزایش تلاش و زحمت‌تراشی برای ارتکاب جرم و افزایش خطرهای مد نظر برای ارتکاب جرم به ترتیب بالاترین تا پایین‌ترین میانگین رتبه‌ای تأثیر در پیشگیری از مسائل فضای مجازی را به خود اختصاص داده‌اند. دیگر اینکه مؤلفه‌های هریک از این ابعاد و تأثیر هریک نیز تعیین شد.

پیشنهادها

همه راهبردهای پیشگیری وضعی از آسیب‌های فضای مجازی با توجه به نظر مثبت کارشناسان نسبت به تأثیر آنها، پیشنهاد می‌شوند.

ـ لزوم بررسی نقش و وظایف سازمان‌های متولی امر پیشگیری از آسیب‌ها، تهدیدها و جرایم فضای مجازی و بازنگری در نقش آنان به نحوی که ضمن هم‌افزایی، هماهنگی مناسبی میان فعالیت‌های آنان برقرار باشد و سلسله‌مراتب مناسبی برای راهبری، هدایت و مدیریت امور پیشگیری برقرار شود.

ـ ضرورت تدوین راهبردهای ناجا در فضای مجازی مبتنی بر بررسی فرصت‌ها، تهدیدها، نقاط قوت و نقاط ضعف ناجا در مواجهه با فضای مجازی؛

ـ اختصاص یک شبکه تلویزیونی به ناجا برای تعامل با جامعه به منظور آگاه‌سازی جامعه از مسائل فضای مجازی و آموزش محافظت از خود و خانواده در فضای مجازی؛

ـ در برنامه‌های پیشگیری، مشارکت همه افراد و نهادهای دارای مهارت و مسئولیت در زمینه پیشگیری از جرم، امری اجتناب‌ناپذیر است.

ـ ایفای نقش ناجا به عنوان یکی از مراجع تأیید صلاحیت در استفاده از امکانات فناوری اطلاعات مانند موبایل، ارائه همه خدمات الکترونیکی مانند عابر بانک و اینترنت بانک و اینترنت به افراد بر مبنای تأیید مراجع ذی‌صلاح از جمله ناجا؛

ـ ایجاد یک رویه برای تعیین صلاحیت وب سایت‌ها، وبلاگ‌ها و ... توسط مراجع ذی‌صلاح از جمله ناجا و درج نمادی در وبلاگ، وب سایت و .... که نشان‌دهنده واجد شرایط بودن آنهاست. سایت‌ها، وبلاگ و ... مکلف به معرفی خود با نشان‌های مصوب شوند و صحت

ادعای آنان توسط پلیس و مراجع ذی‌صلاح بررسی شود و در صورت مجاز بودن توسط کاربران استفاده شوند.

ـ کنترل و نظارت بر سایت‌ها، وبلاگ‌ها، میزبان‌ها و ... از طریق مراجعه و کنترل محتوا و ترافیک ورودی/ خروجی آنها؛

ـ هماهنگی با وزارت فناوری اطلاعات در خصوص فیلتر کردن/ از کار انداختن سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی خلاف شئونات و قوانین جامعه، معاند و ضد دین و مستهجن و سایت‌ها؛

ـ کنترل و نظارت بر همه مطالب موجود در وب سایت‌ها، وبلاگ‌ها و شبکه‌های اجتماعی داخل کشور از بعد جرم؛

ـ کنترل و نظارت بر فعالیت شبکه‌های ارتباطی، وب سایت‌ها و ارائه‌دهندگان خدمات اینترنت و بررسی ترافیک آنها.

منابع فارسی

ابراهیم پور کومله، سمیرا (۱۳۹۱)، «آسیب‌های نوپدید شبکه‌های اجتماعی مجازی در کمین خانواده ایرانی»، نخستین کنگره فضای مجازی و آسیب‌های اجتماعی نوپدید.

پیز، کن (۱۳۸۳)، «جایگاه پیشگیری نخستین از جرم در انگلستان»، مترجم مهدی صبوری پور، تهران: **مجله حقوقی دادگستری**، ش ۴۷، تابستان.

پیکا، ژرژ (۱۳۷۶)، «پیشگیری از جرم‌های شهرنشینی»، ترجمه عزیز طوسی، **ماهنامه دادرسی**، ش ۲، تهران: سازمان قضایی نیروهای مسلح.

جلالی فراهانی، امیرحسین (۱۳۸۴)، «پیشگیری وضعی از جرایم سایبر در پرتو موازین حقوق بشر»، **مجله فقه و اصول**، ش ۶.

جلالی فراهانی، امیرحسین و رضا باقری اصل (۱۳۸۶)، «پیشگیری اجتماعی از جرایم و انحرافات سایبری»، **مجله مجلس و راهبرد**، ش ۵۵.

جلالی، علی‌اکبر (۱۳۸۲)، **آسیب‌شناسی فناوری اطلاعات در خانواده**، تهران: پژوهشکده خانواده.

جلالی، علی‌اکبر (۱۳۸۹)، «نظارت همگانی عامل پیشگیری جرایم در فضای مجازی»، **فصلنامه علمی- ترویجی کارآگاه**، ش ۱۲، دوره دوم.

جلالی، علی‌اکبر (۱۳۸۹)، «نظارت همگانی عامل پیشگیری جرایم در فضای مجازی»، **فصلنامه علمی ترویجی کارآگاه**.

الحسینی، نجمه (۱۳۹۲)، «فضای مجازی، فضایی با فرصت‌ها و تهدیدات بسیار»، روزنامه **رسالت**، س ۲۸، ش ۷۹۴۳.

خلیلی پور رکن آبادی، علی، و یاسر نورعلی وند (۱۳۹۱)، تهدیدات سایبری و تأثیر آن بر امنیت ملی، **فصلنامه مطالعات راهبردی**، س ۱۵، ش ۲.

رزنبام، دنیس و همکاران (۱۳۷۹)، «پیشگیری وضعی از جرم»، ترجمه رضا پرویزی، **مجله حقوقی و قضایی دادگستری**.

زینالی، حمزه (۱۳۸۱)، «پیشگیری از بزهکاری و مدیریت آن در پرتو قوانین و مقررات جاری ایران»، **فصلنامه رفاه اجتماعی**، س ۲، ش ۶.

شاکری، ابوالحسن (۱۳۸۲)، «قوه قضاییه و پیشگیری از وقوع جرم»، **مجموعه مقالات همایش کاربردی پیشگیری از جرم: پلیس پیشگیری نیروی انتظامی**.

شاه محمدی، غلامرضا (۱۳۹۲)، **نقش ناجا در پیشگیری از آسیب‌ها، تهدیدها و کلاهبرداری‌های فضای مجازی**، پروژه تحقیقاتی، تهران: معاونت پژوهش دانشگاه علوم انتظامی امین.

شاه محمدی، غلامرضا و منصور تاهو (۱۳۹۳)، «بررسی شیوه‌های پیشگیری از جرایم سایبری؛ مبتنی بر فناوری اطلاعات»، **فصلنامه علمی پژوهشی پژوهش‌های اطلاعاتی و جنایی**، ش ۳۵، دوره نهم.

صفاری، علی (۱۳۸۰)، «مبانی نظری پیشگیری وضعی»، تهران: **مجلهٔ تحقیقات حقوقی**، ش ۳۳-۳۴.

طارمی، محمدحسین (۱۳۸۷)، «فضای سایبر، آسیب‌ها و مخاطرات، رهاورد نور»، **فصلنامه اطلاع‌رسانی، پژوهشی و مطالعات رایانه‌ای علوم اسلامی**، ش ۲۲.

طاهری گلوندانی، رقیه (۱۳۹۱)، «اینترنت و آسیب‌های اجتماعی»، **نخستین کنگره ملی فضای مجازی و آسیب‌های اجتماعی نوپدید**.

عاملی، سیدسعیدرضا (۱۳۹۰)، **رویکرد دو فضایی به آسیب‌ها، جرایم، قوانین و سیاست‌های فضای مجازی**، مؤسسه انتشارات امیرکبیر.

عمید، حسن (۱۳۷۹)، **فرهنگ فارسی عمید**، تهران: نشر امیرکبیر.

کوسن، موریس (۱۳۷۹)، «نظارت ویدیویی: دلایل موفقیت و شکست»، ترجمه شهرام ابراهیمی، **مجله تخصصی الهیات و حقوق**، ش ۱۵ و ۱۶، بهار و تابستان.

گسن، ریموند (۱۳۷۰)، **جرم‌شناسی کاربردی**، ترجمه مهدی کی نیا، تهران: نشر مترجم.

گسن، ریموند (۱۳۷۶)، «روابط میان پیشگیری وضعی و کنترل جرم»، ترجمه علی حسین نجفی ابرندآبادی، **مجله تحقیقات حقوقی**، دانشگاه شهید بهشتی، ش ۲۰ و ۱۹.

محمدنسل، غلامرضا (۱۳۸۶)، **پلیس و سیاست پیشگیری از جرم**، تهران: دفتر تحقیقات کاربردی پلیس پیشگیری ناجا، انتشارات معاونت تربیت و آموزش ناجا.

میرمحمد صادقی، حسین (۱۳۸۲)، «پیشگیری از وقوع جرم»، **فصلنامه مطالعات امنیت اجتماعی**، پیش‌شماره دوم.

نجاتی حسینی، سید محمود (۱۳۸۰)، **اطلاع‌رسانی و فرهنگ**، انتشارات خانه کتاب.

نجفی ابرندآبادی، علی حسین (۱۳۷۵)، **تحولات جرم‌شناسی**، تهران: انتشارات دانشگاه شهید بهشتی.

نجفی ابرندآبادی، علی‌حسین (۱۳۷۸)، «پیشگیری از بزهکاری و پلیس محلی»، **مجله تحقیقات حقوقی دانشگاه شهید بهشتی**، ش ۲۵-۲۶.

نوری، اعظم و سید کاظم سید باقری (۱۳۹۱)، «واکاوی آسیب‌های بهره‌گیری از اینترنت در فرهنگ اسلامی»، **طهورا**، فصلنامه‌ای در عرصه مطالعات زنان و خانواده.

هادیانفر (۱۳۹۴)، «نشست خبری رئیس پلیس فتا ناجا»، روزنامه سراسری **صبح ایران امتیاز**، صفحه اجتماعی، ۱۷ آذر.

منابع لاتین

Cornish, D. and Clarke, R.(2003),” Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley’s Critique of Situational Crime Prevention”, In ***Theory for Practice in Situational Crime Prevention***, Crime Prevention Studies, (Vol 16) M. Smith and D. Cornish, Eds, Criminal Justice Press, New York.

Lord, Kristin M. & Sharp, Travis (2011), “America’s Cyber Future Security and Prosperity in

the Information Age”, ***Center for a New American Security***, Volume I.