

فهرست مطالب

صفحه	عنوان
۱	پیشگفتار
۵	فصل اول: ماهیت جرایم سایبری و پیشگیری از آن
۶	۱-۱. ماهیت و مفهوم پیشگیری
۷	۱-۱-۱. پیشگیری کیفری
۷	۱-۱-۲. پیشگیری غیر کیفری
۸	۱-۲. انواع پیشگیری
۹	۱-۲-۱. پیشگیری اولیه
۹	۱-۲-۲. پیشگیری ثانویه
۱۰	۱-۲-۳. پیشگیری ثالث
۱۰	۱-۳-۲-۱. پیشگیری جامعه مدار
۱۲	۱-۳-۲-۲. پیشگیری رشد مدار
۱۲	۱-۳-۲-۳. پیشگیری وضعی
۱۴	۱-۳-۲-۴. استراتژی خانواده گرا

۱-۳-۱	مفهوم جرایم فضای مجازی و فواید جرم انگاری آن	۱۴
۱-۳-۱	مفهوم جرایم مرتبط با فضای مجازی	۱۵
۱-۳-۲	فواید جرم انگاری سوء استفاده از داده‌های رایانه‌ای	۱۷
۱-۳-۲-۱	غیر اخلاقی بودن تخلفات مرتبط با رایانه	۱۷
۱-۳-۲-۲	مقایسه خسارت داده با خسارت اموال فیزیکی	۱۷
۱-۳-۲-۳	تشویق نوآوری	۱۸
۱-۳-۲-۴	کافی نبودن قواعد مسئولیت مدنی	۱۸
۱-۳-۲-۵	هزینه دعوای حقوقی	۱۹
۱-۴-۱	جنبه‌های حقوقی جرایم مرتبط با فضای مجازی	۱۹
۱-۴-۱	سرقت در فضای مجازی	۲۰
۱-۴-۱-۱	ربودن	۲۲
۱-۴-۱-۲	تصاحب	۲۳
۱-۴-۱-۳	قصد محروم کردن دائمی مالک	۲۴
۱-۴-۲	پولشویی	۲۶
۱-۴-۳	تأمین مالی فعالیت‌های تروریستی	۲۸
۱-۴-۴	دسترسی غیرمجاز	۲۹
۱-۴-۵	جعل رایانه‌ای	۳۱
۱-۴-۶	رمزگیری	۳۴
۱-۴-۷	سرقت هویت	۳۷
۱-۴-۸	کلاهبرداری	۳۹
۱-۴-۹	تخریب و اخلاف در داده‌ها یا سامانه‌های الکترونیکی	۴۱
۱-۴-۱۰	افشای داده‌ها و تعرض به حریم خصوصی	۴۲
۱-۴-۱۱	هرزه نگاری در فضای مجازی	۴۴
۱-۴-۱۲	نقض حقوق کودک در فضای مجازی	۴۶
۱-۵-۵	شئون انسانی در فضای مجازی	۵۰
۱-۵-۱	مفهوم شئون انسانی	۵۰

۵۳	۱-۵-۲. محورهای شئون انسانی.....
۵۹	۱-۵-۳. سازوکارهای تضمین شئون انسانی در فضای مجازی.....
۶۹	۱-۶. توسعه حقوق و رعایت اخلاق در محیط سایبری.....
۶۹	۱-۶-۱. هویت در فضای مجازی.....
۷۰	۱-۶-۱-۱. چستی هویت در جهان واقعی.....
۷۲	۱-۶-۱-۲. مفهوم هویت در فضای مجازی.....
۷۵	۱-۶-۲. چالش‌های اخلاقی در فضای سایبر.....
۷۷	۱-۶-۲-۱. چالش‌های هویت دیجیتال.....
۷۹	۱-۶-۲-۲. دزدی هویت در فضای مجازی.....
۸۲	۱-۶-۳. مدیریت هویت در فضای مجازی.....

فصل دوم:

۸۵	اقدامات امنیتی و پیشگیرانه در جهت کاهش جرایم در شبکه‌های اجتماعی و فضای مجازی
۸۶	۱-۲. اهداف و محدوده سیاست‌های امنیتی.....
۸۶	۱-۲-۱. اهداف مورد نظر.....
۸۷	۱-۲-۲. تهدیداتی که باید مدنظر قرار گیرد.....
۸۷	۲-۲. ایجاد سیاست امنیتی.....
۸۷	۱-۲-۲. ضرورت وجود سازمان اطلاع رسانی و گروه ضربت.....
۸۸	۲-۲-۲. تعیین تدابیر امنیتی.....
۸۸	۱-۲-۲-۲. تشخیص و ارزیابی دارایی‌ها.....
۸۹	۲-۲-۲-۲. ارزیابی خطرات.....
۹۰	۳-۲-۲-۲. گزینش تدابیر امنیتی کارآمد.....
۹۰	۳-۲-۲. آزمایش سیستم و اعمال اقدامات بازدارنده ممکن.....
۹۱	۱-۳-۲-۲. اقدامات بازدارنده سازمانی افراد خرابکار.....

۲-۲-۳-۲	اقدامات بازدارنده در مقابل مجرمین	۹۲
۲-۲-۳-۳	در حوزه برنامه نویسی سیستم و برنامه نویسی کاربردی	۹۴
۲-۲-۳-۳	استراق سمع و دیگر روشهای فنی	۹۴
۲-۲-۳-۴	اجرا، کنترل و بهنگام سازی سیستمهای ایمنی	۹۴
۲-۳-۳	عناصر اصلی سیستم ایمنی مؤثر	۹۶
۲-۳-۱	اقدامات ایمنی شخصی و آموزشی	۹۶
۲-۳-۱-۱	کنترلها	۹۶
۲-۳-۱-۲	ایجاد انگیزه، آموزش و قوانین اخلاقی	۹۷
۲-۳-۲	اقدامات ایمنی فیزیکی	۹۸
۲-۳-۱-۲	طرح معماری	۹۸
۲-۳-۲-۲	مواد و تجهیزات ساختمانی	۹۹
۲-۳-۳	معیارهای ایمنی فنی و سازمانی	۹۹
۲-۳-۳-۱	معیارهای کنترل عمومی	۱۰۰
۲-۳-۳-۲	کنترل‌های ویژه ورودی	۱۰۳
۲-۳-۳-۳	کنترل‌های ارتباطی ویژه	۱۰۳
۲-۳-۳-۴	کنترل‌های پردازشی ویژه	۱۰۴
۲-۳-۳-۵	کنترل‌های ویژه ذخیره اطلاعات	۱۰۵
۲-۳-۳-۶	کنترل‌های ویژه خروجی	۱۰۶
۲-۳-۳-۷	محافظت ویژه از برنامه‌های پروانه دار	۱۰۶
۲-۳-۴	بازرسی داخلی	۱۰۸
۲-۳-۵	بیمه‌های مربوط به جرایم کامپیوتری	۱۰۹
۲-۳-۶	تنظیم قراردادها	۱۰۹
۲-۳-۷	اقدامات قانونی ضروری در صورت بروز موارد مشکوک و ورود خسارت	۱۱۰
۲-۴	ابعاد بین المللی	۱۱۱
۲-۵	صلاحیت کیفری در جرائم سایبری	۱۱۱
۲-۶	چالش‌های قواعد دادرسی سنتی در فضای سایبر	۱۱۲

فصل سوم: نتیجه گیری ۱۲۱

۱-۳. نتیجه گیری ۱۲۲

۲-۳. پیشنهادات ۱۲۵

منابع ۱۲۷

الف) کتب فارسی ۱۲۷

ب) مجلات و نشریات ۱۳۱

ج) پایان نامه‌ها ۱۳۱

منابع انگلیسی ۱۳۳

پیشگیری از وقوع جرم در فضای مجازی مهم‌ترین اولویت پلیس فتا ست و فضای سایبری در این راستا به صورت روزانه و مستمر توسط پلیس فتا رصد می‌شود، عدم آگاهی و دانش فنی کاربران دلیل اصلی وقوع جرایم در فضاهای مجازی است که انتظار می‌رود صدا و سیما و رسانه‌ها بیشتر از گذشته به بحث آگاه‌سازی مردم ورود پیدا کنند و خانواده‌ها نیز تا جایی که امکان دارد از فضای مجازی استفاده نکنند و اگر لازم بود بر اساس نیاز بستر دسترسی به فضاهای مجازی را برای فرزندان خود فراهم کنند و بر رفتار آنان کنترل داشته باشند تا دچار مشکل نشوند.

فکر ایجاد شبکه، پیش از دهه ۶۰ و با این مضمون به وجود آمد که چگونه می‌توانیم بیت‌های اطلاعاتی را روی یک رسانه ارتباطی به صورتی کارا و قابل اعتماد ارسال کنیم. پس از آن، با تحولاتی که در این زمینه به وجود آمد از اواسط دهه ۷۰ تلاش شد تا سرویس‌های ارتباطی را روی یک مجموعه از شبکه‌های به هم متصل تدارک ببینند. به این ترتیب، سنگ بنای تبادل وسیع و هماهنگ « داده » که امروزه یکی از بخشهای مهم کار با رایانه است، گذاشته شد این فناوری جدید « ارتباط بین شبکه‌ای » نام دارد. اینترنت نیز، مانند سایر محصولات اساسی انفورماتیک از بطن فعالیتهای نظامی زاده شد. ابتدا در سال ۱۹۶۹ وزارت دفاع آمریکا شبکه‌ای بنام « آرپانت » ایجاد کرد که چهار رایانه را به هم متصل می‌کرد. در سال ۱۹۷۲ این شبکه در معرض دید همگان قرار گرفت و بسیاری از دانشگاه‌ها و موسسه‌های پژوهشی به آن پیوستند.

یکی از دشواری‌های بشر در توسعه دانش و بکارگیری همه جانبه آن، کندی پردازش اطلاعات، بعنوان محتوای تشکیل دهنده دانش و همچنین محدودیت‌های بسیار در جابجایی و نگهداری و ذخیره سازی آن است. به همین منظور، یکی از آرزوهای انسان، دستیابی به امکاناتی بود که بتواند این موانع را از پیش رویش بردارد. تقریباً در

ابتدای قرن بیستم، این آرزو تحقق یافت و فناوری رایانه به عنوان ابزاری حسابگر و پردازش گر تقدیم جامعه بشری شد، بنابراین سیستم‌ها و ابزارهای رایانه‌ای در بستر شبکه‌های رایانه‌ای ارتقاء یافتند و سرانجام، در ابتدای دهه ۱۹۹۰ نخستین شبکه جهانی، به نام شبکه جهانی وب پدید آمد. این شبکه، در واقع، ویترونی از داده‌های دسترس پذیر در سراسر جهان بود؛ هر چند هنوز محدودیت‌های بسیاری را پیش روی خود می‌دید.

جهان مجازی شکل دیگری از جهان واقعی است که بر فراز آن قرار گرفته است. به کار بردن عباراتی چون دولت مجازی، پست الکترونیک، جرم الکترونیک، جرم اینترنتی، تجارت اینترنتی، دوستی مجازی و مانند آن، که همگی در درجه اول اشاره به جهان مجازی دارند، نشان دهنده تشابه میان عناصر هر یک از این دو جهان است. اگرچه توسعه تکنولوژی‌های ارتباطی و شکل گیری جهان مجازی، نتایج و آثار مثبت بسیاری در جهت پیشرفت جوامع بشری داشته است، نمی‌تواند تنها دربر گیرنده نقاط مثبت باشد. در این جهان هم همچون جهان واقعی ابعاد منفی و مرضی وجود دارد. یکی از این ابعاد وجود جرم، کلاهبرداری و جنایت هست.

در فضای ارتباطی جدید، عامل زمان و مکان کم رنگ شده است و دوری و نزدیکی به عنوان عامل خنثی در ارتباطات محلی و جهانی محسوب می‌شوند. در واقع جهان جدیدی به موازات جهان واقعی به وجود آمده است که جهان بی مرز، جهان بی مکان، به تعبیر دقیق تر جهان مجازی نام گرفته است.

پدیده جرایم رایانه‌ای مرز نمی‌شناسد. با افزایش گسترش و بکارگیری فناوری‌های جدید، پدیده جرایم مرتبط با این فناوری‌ها نیز به سرعت و تصاعدی افزایش می‌یابند. هم اکنون مجرمان به ویژه در کشورهای پیشرفته کمتر به خودشان زحمت می‌دهند به بانکی، مسلحانه دستبرد بزنند و خطر دستگیری و زندانی شدند و مرگ را به جان بخرند آنان قادرند از خانه خود و با کمی امکانات، پول بانک‌ها را از نقطه‌ای به نقطه دیگر جهان انتقال دهند و احیاناً در امور مختلف به کار می‌گیرند. این در حالی است که آنان سعی می‌کنند با اقدامات بسیار پیچیده از خود ردپایی به جای نگذارند. در ایران نیز سال‌ها استفاده از رایانه و اینترنت روند روبه گسترش داشته است، گسترش روزافزون جرایم رایانه‌ای در ایران مانند سرقت از کارت‌های اعتباری، سرقت اینترنتی، سرقت از دستگاه‌های خودپرداز (عابر بانک)، نفوذ در شبکه‌های اطلاعاتی موسسات دولتی و خصوصی و احیاناً تخریب یا سوء استفاده مالی، هرزه نگاری اینترنتی و ... ایجاب می‌نماید، کارشناسان علوم مختلف رایانه‌ها، شبکه‌ها و اینترنت، پلیس و ... به آخرین یافته‌های این علم تجهیز شوند تا بتوانند با این نوع جرایم مقابله نمایند. از این رو اطلاع و

آگاهی از آخرین شیوه‌های تخریبی و مجرمانه رایانه‌ای برای پیشگیری، ردیابی و پی جویی و کنترل این نوع جرایم کاملاً ضروری می‌باشد.

پیش از آنکه متناسب با شرایط خاص و متمایز فضای سایبر، هنجارهای لازم وضع و نهادینه شود، هنجارشکنان به این فضا راه یافته و رها شده‌اند. از سوی دیگر، هنجارهای موضوعه در دنیای فیزیکی کارایی و اثر بخشی لازم در دنیای سایبر را ندارند. پس، امکان نقض آسان این هنجارها فراهم است؛ بدون آنکه دغدغه‌های ناشی از گرفتاری در بند ضمانت اجراهای کیفری و غیرکیفری وجود داشته باشد.

از طرفی، فضای سایبری با برخورداری از ویژگی‌های منحصر به فردی چون بدون مرز بودن، امکان هنجارشکنی را به تمامی نقاط دنیا گسترش داده است. همچنین با گمنام سازی کاربرهای سایبری، امکان شناسایی هویت هنجارشکنان، تعقیب و پیگرد آن‌ها را با مشکلات جدی مواجه کرده است.

بنابراین ضرورت دارد فضای سایبر را تبیین نموده و سعی داریم راهکارهای لازم و ضروری پیشگیری از جرم در فضای مجازی را جهت سیاست گذاری اجتماعی ارائه نماییم.