پژوهشنامه حقوق فارس، سال اول، شماره اول، زمستان ۱۳۹۷

تدابیر پیشگیرانه فنی جهت حفاظت از اطلاعات مالی در فضای سایبر

الهام سلیمان دهکردی[۱]، زهرا صالح آبادی [۲]، کیانوش سمنگوئی[۳]

چکیده

صیانت از اطلاعات مالی از مولفه‌های راهبردی تامین امنیت در فضای سایبر است. اشخاص سودجو همواره درصدد اند برای تحقق نیات سوء خود از این اطلاعات در فضای سایبر بهره برده و از این طریق به سودهای کلانی دست یابند لذا ضروری است به منظور کاهش تهدیدات علیه این اطلاعات به تدابیر پیشگیرانه فنی مبادرت ورزید. این تدابیر برای حفاظت از اطلاعات مالی بیشتر استفاده می‌شوند چرا که اکثر تهدیدات علیه این اطلاعات به شیوه‌های فنی چون مهندسی اجتماعی صورت می‌گیرد و دارای ماهیت تخصصی است. در فرآیند مقرره گذاری نیز قانون گذار با این نوع از تدابیر بیگانه نبوده و در برخی موارد به طور صریح و در برخی به طور ضمنی به این تدابیر پرداخته است. پلیس فتا نیز به عنوان تنها نهاد پلیسی فعال در این حوزه به این گونه تدابیر وقعی ننهاده است. مراکز فعال در حوزه امنیت سایبری همچون آپا و ماهر نیز رویکرد یکسانی در این خصوص اتخاذ نکرده اند، مرکز آپا بخش عمده‌ای از تدابیر خود را در حوزه فنی ساماندهی نموده در حالی که مرکز ماهر به این تدابیر توجهی ننموده است.

واژگان کلیدی: فضای سایبری، مقرره گذاری، مرکز آپا، مرکز ماهر، پلیس فتا.

۱- دکتری حقوق کیفری و جرم شناسی از دانشگاه علامه طباطبایی soleiman.elham@gmail.com
۲- دانشجوی دکتری حقوق کیفری و جرم شناسی دانشگاه فردوسی مشهد و مدرس دانشگاه(نویسنده مسئول) salehabadi.zahra@gmail.com
۳- دانشجوی دکتری حقوق کیفری و جرم شناسی kia_samangooei34@yahoo.com

مقدمه

اطلاعات مالی سایبری جوهره اصلی فضای تبادل اطلاعات است. حفظ صحت و محرمانگی این اطلاعات نشانگر استواری فضای سایبر و ارزشمندی این اطلاعات است. این اطلاعات از مرحله ورود در فضای سایبر تا خروج از این فضا در معرض انواع رفتارهای مخرب و مختل کننده قرار می‌گیرند که این رفتارها موجب نابودی، افشاء و یا تغییر آن‌ها می‌شود. تنها در یک صورت می‌توان تهدیدات علیه این اطلاعات را کاهش داد و به تبع ارزشمندی آن‌ها را در فضای سایبری تامین نمود و آن در صورتی است که از تدابیر فنی پیشگیری وضعی استفاده گردد. این تدابیر بر خلاف تدابیر نظارت انسانی هم سنخ و هم جنس با اقدامات افراد تدابیر دارای چهار گروه برنامه است: نخست تدابیر محدود کننده یا سلب کننده دسترسی، دوم تدابیر رمزنگارها، سوم تدابیر صدور مجوز و چهارم تدابیر نظارتی. در برنامه نخست دسترسی به اطلاعات مالی دشوار یا غیرممکن می‌شود. در برنامه دوم ماهیت اصلی اطلاعات مالی پنهان یا غیرقابل درک می‌شود، در برنامه سوم تنها به افراد مجاز اجازه ورود به پایگاه اطلاعات مالی داده می‌شود و در برنامه چهارم با نظارت بر ورودی و خروجی‌ها از ورود یا خروج اطلاعات مالی جلوگیری می‌شود. در مقررات موجود در حوزه سایبر هر چند تا اندازه‌ای به این تدابیر توجه شده اما برای حفاظت از اطلاعات مالی نیست دلیل این امر این است که وصفی به نام اطلاعات مالی برای قانون گذار ناشناخته بوده است. برخی مراکز حامی امنیت سایبری نیز تنها برای حفاظت از حریم خصوصی شهروندان از این تدابیر استفاده کرده اند و توجهی به اطلاعات مالی نداشته اند. پلیس فتا نیز اصلا به این تدابیر توجهی ننموده است و تنها شهروندان را از شیوه‌های جدیدی که رخنه گران برای نقض حریم اطلاعاتی استفاده می‌کنند، آگاه ساخته است. در ادامه نخست به ماهیت پیشگیری وضعی با اتخاذ تدابیر نظارت فنی پرداخته و جایگاه آن را در مقررات تبیین نموده، سپس به عملکرد مراکز فعال در این حوزه پرداخته و در پایان به تبیین شیوه‌های تدابیر فنی پرداخته ایم.

۱-پیشگیری وضعی با اتخاذ تدابیر فنی

پیشگیری وضعی رویکردی است که با تمرکز بر محیط هایی که جرم در آن محقق می‌شود تنها به دنبال کاهش فرصت‌های مجرمانه و ایجاد تغییر در آن‌ها است. منظور از ایجاد تغییر، جاذبه زدایی از سیبل جرم، بالا بردن هزینه، سخت کردن ارتکاب جرم و خطرناک کردن آن است(صفاری،۱۳۸۰،۱٤). در این نوع از پیشگیری جهت افزایش هزینه جرم و حفظ آماج جرم اقداماتی صورت می‌گیرد که این اقدامات دارای اشکالی است. از جمله این اشکال می‌توان به استفاده از شیوه‌های سنتی نظارت و کنترل، حفاظت‌های فیزیکی و اقدامات مادی، کنترل ورودی‌ها و خروجی ها، کنترل ابزاری که ارتکاب جرم را تسهیل می‌کند، ایجاد مانع برای برقراری تماس بین بزهکار بالقوه و آماج جرم اشاره کرد. در فضای واقعی برای حفاظت از سیبل جرم از تدابیر فیزیکی و سنتی کنترل استفاده می‌شود که ماهیتا ملموس و عینی هستند و دارای ماهیت چندان پیچیده و تخصصی نیستند مثلا با نصب دزدگیر بر روی خودرو از سرقت آن جلوگیری می‌شود اما در فضای سایبر برای حفاظت از سیبل جرم می‌بایست از تدابیر فنی امنیتی متناسب با این فضا و از جنس آن استفاده شود که بیشتر این تدابیر ناظر به کنترل ورودی و خروجی‌ها و کنترل ابزاری است که ارتکاب جرم را تسهیل می‌کند و دارای ماهیتی فنی است (خانعلی پور،۱۳۹۰،۱۷). دلیل این تفاوت ناشی از دو امر است؛ نخست این که فضای سایبر دارای ماهیتی تخصصی است و افراد سودجو جهت نقض حریم اطلاعاتی اشخاص در این فضا از اقدامات فنی متناسب با آن استفاده می‌کنند. اکثر رفتارهای ناقضانه‌ای که علیه اطلاعات مالی اشخاص در این فضا صورت می‌گیرد مقید به وسیله است و بدون استفاده از وسیله که در این جا رایانه وسیله است، امکان پذیر نمی‌باشد، در نتیجه با اعمال محدودیت‌های لازم بر وسیله می‌توان از ارتکاب رفتارهای مجرمانه علیه اطلاعات مالی جلوگیری نمود این امر امتیازی برای پیشگیری وضعی با اتخاذ تدابیر فنی از جرایم سایبری محسوب می‌شود که پیشگیری وضعی از جرایم سنتی از آن بی بهره است زیرا در جرایم سنتی کمتر عامل موثری را می‌توان میان آماج جرم و مجرم قرار داد در حالی که مقید به وسیله بودن جرایم رایانه‌ای و امکان ساماندهی و تنظیم ارتباطات، امکان کنترل ابزارهای ارتکاب جرم را فراهم نموده است. دوم فضای سایبر

به اقتضای ویژگی‌های خاصی که دارد برای پیشگیری وضعی با اتخاذ تدابیر فنی مناسب تر است. از جمله این ویژگی‌ها می‌توان به گستردگی خسارتی که از اقدام فرد رخنه گر حاصل می‌شود، آسیب پذیر بودن اطلاعات مالی به عنوان آماج جرم، رهایی بستر سایبری و استفاده خود مرتکبان از شیوه‌های فنی جهت نقض حریم‌های اطلاعاتی اشاره کرد(خالقی پوستچی،۱۳۸۸،۱۲).

آسیب پذیری اطلاعات مالی در این فضا از چند جنبه است؛ نخست ارزشمند بودن اطلاعات که معیار این امر شخصی است. فضای سایبر که سرشار از اطلاعات متنوع و گران بها است می‌تواند افراد با انگیزه‌های مختلف را به سوی خود جذب کند که مهم ترین انگیزه برای جذب افراد انگیزه مالی می‌باشد. این اطلاعات همواره به لحاظ ارزشمند بودن، آماج جرم قرار گرفته و یا زمینه ارتکاب دیگر جرایم را فراهم می‌سازند. افراد سودجو اغلب برای دسترسی به این اطلاعات از شیوه هایی چون فیشینگ، اسکیمر، فارمینگ و ... که شیوه‌های فنی هستند، بهره برده و سپس اقدام به سرقت این اطلاعات، کلاهبرداری به وسیله این اطلاعات، اخلال، تخریب، محو و جعل آن‌ها می‌کنند بنابراین ضروری است تدابیری که جهت حفاظت از اطلاعات مالی اشخاص در این فضا صورت می‌گیرد تخصصی بوده تا کارایی لازم را داشته باشد و بتواند از آن سیبل به خوبی حفاظت کند. مقاوم پذیری اطلاعات مالی: هر چه از یک هدف حفاظت بیشتری شود، آن هدف امن تر می‌شود و به راحتی در معرض حمله قرار نمی‌گیرد از این رو هر چه از اطلاعات باارزش افراد اقدامات حفاظتی متناسب با ماهیت اطلاعات در این فضا به عمل آید، اطلاعات مقاوم پذیرتر می‌شوند و به آسانی مورد حمله قرار نمی‌گیرند. منظور از اقدامات حفاظتی متناسب با این فضا اقدامات فنی است که از جنس اقدامات خود فرد رخنه گر است و دارای ماهیتی فنی و تخصصی است. رویت پذیری اطلاعات مالی: اطلاعات مالی نباید به سهولت در معرض دید افراد سودجو قرار گیرند چرا که در این هنگام آن‌ها به سمت اطلاعاتی که ملاحظه نموده اند حمله ور شده و ارزشمندی آن‌ها را از بین می‌برند(جلالی فراهانی،۱۳۸۸،۹). حفاظت فنی از این اطلاعات نیز با سه معیار مهم تبلور می‌یابد: نخست محرمانگی تا به واسطه آن اطلاعات به صورت غیرمجاز افشاء نشوند، دوم صحت و تمامیت تا از تغییر و یا حذف غیرمجاز آن‌ها پیشگیری شود و سوم قابلیت دسترسی تا با تحقق آن

ممانعت غیرمجاز از دسترسی به اطلاعات پیش نیاید. غیر از این سه معیار باید معیارهای قابل استناد بودن این اطلاعات و انکارناپذیری اطلاعات نیز مدنظر قرار بگیرد تا به جهت شکلی نیز حفاظت از این اطلاعات به درستی تضمین شود(عالی پور،۱۳۹۰، ٤٠).

استفاده از تدابیر پیشگیری اجتماعی در این خصوص چندان راهگشا نیست و توصیه نمی‌شود زیرا این تدابیر بر روی زمینه‌های ارتکاب جرم تمرکز می‌کند و در بلند مدت جواب می‌دهد در حالی که سارقان اطلاعات مالی با استفاده از موقعیت‌های جرم زا به صورت آنی دست به ارتکاب جرم می‌زند از این رو نیاز به تدابیر فنی بیش از پیش احساس می‌شود تا دسترسی به اطلاعات مالی به طور غیرمجاز، غیرممکن یا حداقل دشوار شود. این تدابیر به چهار نوع تدابیر محدود کننده یا سلب کننده دسترسی، تدابیر ناشناس کننده و رمزنگارها، تدابیر صدور مجوز و تدابیر نظارتی تقسیم می‌شوند.

۲- جایگاه پیشگیری فنی در مقررات

در مصوبات موجود در حوزه فضای سایبری و قوانین موجود در این راستا قانون گذار گاه به طور ضمنی و گاه به طور صریح به استفاده از تدابیر فنی جهت تحقق امنیت فضای سایبر پرداخته که به آن‌ها اشاره می‌شود. نخست مصوبات شورای عالی فضای مجازی است. این شورا به تاریخ ۱۷ اسفند ۱۳۹۰ به فرمان مقام معظم رهبری تشکیل شد و موظف گردید تا بر فضای درونی و بیرونی اینترنت به طور کامل و به روز اشراف داشته و امنیت این فضا را تامین سازد. در مصوبه این شورا با موضوع توسعه فضای مجازی سالم، مفید و امن به شماره ۹٤/۱۰۰۱۵۱/ش مصوب ۱۳۹٤/۰۱/۳۰ به تعریف فضای مجازی ایمن پرداخته شده است. در این مصوبه آمده: فضای ایمن فضایی است متشکل از شبکه‌های ارتباطی که در آن محتوا و خدمات مفید در چارچوب مبانی و ارزش‌های اسلامی و مقررات کشور ارائه می‌شود و کاربران می‌توانند بر اساس ویژگی‌های جمعیتی از قبیل سن، جنس، شغل و تحصیلات از محتوا و خدمات مورد نیاز بهره مند شوند و حتی الامکان در برابر محتوا و رفتارهای آسیب زا محفوظ بمانند. در عنوان این مصوبه هر چند به توسعه فضای مجازی سالم، مفید و ایمن پرداخته شده است اما در تعریفی که از فضای ایمن ارائه شده، به نظر می‌رسد فضای ایمن به لحاظ محتوایی

مدنظر بوده یعنی فضایی که محتوای آن در چارچوب مبانی اسلامی باشد به عبارت بهتر در این مقرره قانون گذار صرفا به پالایش محتوا توجه داشته در حالی که پالایه یک اقدام حفاظتی محسوب نمی‌شود(فضلی،۱۳۸۹،۱۱۱). دلیل این امر این است که پالایه همواره از سوی مقامات دولتی و برای پاکسازی یک وب سایت از اطلاعاتی که به لحاظ مضمون با مبانی اخلاقی و اسلامی ناسازگاراند به کار رفته و جنبه حفاظتی ندارد در حالی که آن چه در حفاظت از اطلاعات مالی مدنظر است این است که از اطلاعات مالی حفاظت به عمل آید تا این اطلاعات افشاء، تخریب و محو و ... نشوند که این حفاظت می‌تواند هم از سوی اشخاص حقیقی و هم حقوقی باشد. در مصوبه دیگر این شورا با موضوع سیاست‌های ساماندهی خدمات پیامکی ارزش افزوده و پیامک انبوه در شبکه‌های ارتباطی به شماره ی ۹۳/۱۰۳٦۸۱/ش مورخ ۱۳۹۳/۱۱/۰۱ در بند ٤ آمده: به منظور حفظ و صیانت از اطلاعات خصوصی مخاطبان پیام و بر اساس قوانین به ویژه قانون جرائم رایانه‌ای مصوب ۱۳۸۸، ارائه دهندگان خدمات ارتباطی و ارائه دهندگان خدمات محتوایی حق واگذاری، فروش و یا در اختیار قرار دادن این اطلاعات به دیگران را ندارند. در این مصوبه نیز هر چند به حفاظت و حراست از اطلاعات اشاره شده، اما تنها به حفاظت از اطلاعاتی که مربوط به حریم خصوصی شهروندان است، پرداخته شده و به اطلاعات مالی به طور کلی توجهی نشده است(جاوید نیا،۱۳۸۸،۵). دلیل این امر چندان مشخص نیست اما به نظر می‌رسد یا وصف اطلاعات مالی به طور کلی برای مقنن ناشناخته بوده و از این رو حمایتی از این اطلاعات به عمل نیاورده و یا اطلاعات مالی را نیز بخشی از اطلاعات شخصی افراد قلمداد نموده و آن‌ها را همانند اطلاعات شخصی مشمول حمایت قرار داده است. به این استدلال این خدشه وارد می‌شود که از اطلاعات مالی اشخاص حقوقی در این قالب نمی‌توان حفاظت نمود. اقداماتی که جهت حفاظت از اطلاعات شخصی نیز به عمل آمده، تدابیر واسطه‌ای هستند. این تدابیر، تدابیری هستند که در پی تنظیم مقررات مناسب برای حفاظت از اطلاعات اند(جوان جعفری،۱۳۸۹،۵). این تدابیر ناظر به تدابیر پیشگیری وضعی اند که اطلاعات شخصی افراد را که در برخی موارد آماج جرم قرار می‌گیرند، هدف قرار داده که حفاظت از این اطلاعات یا در قالب تدابیر نظارتی انسانی و یا تدابیر نظارتی فنی است که در این نوشته تنها قسم دوم مدنظر است. در مصوبه دیگر این شورا در خصوص طرح‌های کلان

مرکز ملی فضای مجازی کشور جهت تدوین لایحه بودجه و در تصویب نامه این شورا در خصوص شرح وظایف، اختیارات و اعضای کمیسیون عالی فضای مجازی، به ارتقای امنیت سایبری پرداخته شده است، اما هیچ سخنی از چگونگی تامین این مهم به میان نیامده است. در این مصوبه قانون گذار به تولید محتوای فضای مجازی به صراحت توجه نموده است در حالی که مفهوم امنیت و ابعاد آن در این جا تشریح نشده است. از منظر حقوقی امنیت سایبری در دو مفهوم مضیق و موسع به کار می‌رود. در مفهوم مضیق به معنای اتخاذ تدابیر فنی پیشگیرانه برای حفاظت و حراست از اطلاعات در بستر سامانه‌های رایانه‌ای و مخابراتی است(احسانی موید،۱۳۸۹،۱۲). در این مفهوم اقدامات غیرفنی جایگاهی نداشته و اشخاص موضوع مستقیم تدابیر امنیتی قرار نمی‌گیرند اما در مفهوم موسع دو قسم از تدابیر را برای تامین امنیت در محیط سایبر می‌توان برشمرد: الف، تدابیر مستقیم یا اصلی، این تدابیر به کلیه تدابیر فنی و قانونی گفته می‌شود که برای تامین امنیت دو موضوع زیر به کار می‌رود: نخست اطلاعات رایانه‌ای که از مرحله ورود یا تولید تا ذخیره و انتشار و مورد استفاده قرار گرفتن در معرض انواع رفتارهای مخرب و مختل کننده است که این رفتارها موجب نابودی یا افشای اطلاعات مالی در این فضا می‌شود و دوم سیستم‌ها و شبکه‌های رایانه‌ای و مخابراتی، سیستم و شبکه نیز همچون اطلاعات آسیب پذیر بوده و از آن جا که مقوم آن اطلاعات است، اقداماتی نظیر انتشار ویروس، اختلال در کارکرد و بازدهی، ممانعت از ترافیک و دسترسی به اطلاعات و غیره امنیت آن‌ها را به شدت تهدید می‌کند، از این رو برای امنیت اطلاعات و سیستم اقدامات پیشگیرانه فنی مورد استفاده قرار می‌گیرد. امنیت اطلاعات نیز به فرآیند حفاظت از اطلاعات در برابر کارهای غیرمجاز شامل دسترسی، استفاده، افشاء، اختلال، تغییر، مطالعه، بازرسی و ضبط گفته می‌شود(حسن بیگی،۱۳۸٤، ۱۱). هر چند در مقرره پیش گفته امنیت سایبری به گونه‌ای عام مورد استفاده قرار گرفته و اشاره‌ای به تعبیر اطلاعات مالی نشده اما امنیت اطلاعات نیز در گستره امنیت سایبری می‌گنجد و اطلاعات مالی نیز جزء مصادیق آن به شمار می‌آید. در اساسنامه مرکز ملی فضای مجازی در ماده ۲ به مقابله با تهدیدات فضای سایبر با استفاده از تدابیر فنی پرداخته شده است. یکی از مهم ترین تهدیدات در حوزه سایبر تهدیداتی است که علیه محرمانگی و اصالت اطلاعات مالی صورت می‌گیرد. قانون گذار در همین ماده به طور صریح خود به این امر اشاره

کرده که برای از بین بردن تهدیدات مذکور از تدابیر فنی استفاده شود. در مصوبه دیگر این شورا در خصوص تعریف و الزامات حاکم بر تحقق شبکه ملی اطلاعات و بودجه سال ۱۳۹۳ نیز در بند چهارم مقرره دوم به ایجاد شبکه‌ای با قابلیت عرضه انواع خدمات امن اعم از رمزنگاری و امضای دیجیتال پرداخته است. در این مقرره قانون گذار تنها به امنیت شبکه توجه داشته و اشاره‌ای به امنیت اطلاعات نکرده است. امنیت شبکه پردازه‌ای است که طی آن یک شبکه در مقابل انواع مختلف تهدیدات اعم از داخلی و خارجی امن می‌شود به عبارت دیگر امنیت شبکه ناظر بر حفاظت از شبکه در قبال حملات است که گاه این حملات منجر به تخریب کل شبکه و گاه منجر به دسترسی غیرمجاز به منابع و اطلاعات می‌شود، با این حال در امنیت شبکه متخصصان بیشتر بر عملکرد صحیح سیستم کامپیوتری تمرکز دارند در حالی که در امنیت اطلاعات بیشتر تاکید بر حفاظت از اطلاعات خصوصا اطلاعات باارزش اشخاص است تا در پرتو این حفاظت بتوان از ضررهای هنگفتی که ممکن است در اثر رفتارهای مخرب به اشخاص وارد آید جلوگیری نمود. تدابیر پیشنهاد شده در این ماده جهت خدمت رسانی امن به کاربران همگی در قالب تدابیر پیشگیری فنی اند. در این مقرره از میان تدابیر فنی تنها به رمزنگاری و امضای دیجیتال اشاره شده، در حالی که این دو راهکار بیشتر جهت تامین امنیت خود اطلاعات به کار می‌روند و نه شبکه. در معنی یاد شده از این رو بهتر می‌بود مقنن به طور تمثیلی به این تدابیر می‌پرداخت تا لااقل بتواند امنیت شبکه را در قالب این اقدامات به طور کامل تامین سازد. در مصوبه دیگر این شورا تحت عنوان سیاست‌های حاکم بر برنامه‌های رایانه‌ای در بند ۱۰ به حفظ حریم خصوصی و حمایت از حقوق مصرف کننده اشاره شده، اما تدابیر واسطه‌ای پیش بینی شده در این بند نیز تنها ناظر به حفظ حریم خصوصی است و اطلاعات مالی اشخاص حقوقی تحت شمول این مقرره قرار نمی‌گیرند اما حمایت از حقوق مصرف کننده می‌تواند شامل حمایت از اطلاعات مالی مشتریان نیز شود که این مشتریان هم می‌توانند اشخاص حقوقی و اشخاص حقیقی باشند. در مقررات و ضوابط شبکه‌های اطلاع رسانی رایانه مصوب ۱۳۸۰ قانون گذار در بند ب ماده ٦ به استفاده از تدابیر فنی جهت صیانت از شبکه‌ها و اطلاعات پرداخته است. در این بند آمده: سیستم بارو[1] مناسب به منظور صیانت

1 - Firewall

شبکه‌ها از تخریب، فریب و سرقت اطلاعات به کار می‌رود. در این مقرره قانون گذار به امنیت اطلاعات به طور صریح پرداخته است. اطلاعات به کار رفته در این متن مطلق است و شامل اطلاعات مالی و غیرمالی می‌گردد. در این مقرره تنها به حفاظت از اطلاعات در برابر سرقت، تخریب و فریب اشاره شده در حالی که بهتر بود مقنن به حفاظت از اطلاعات در برابر تهدیدات به نحو مطلق اشاره می‌کرد. راهکار فنی ارائه شده در این ماده نیز تنها فایروال است و مقنن به سایر تدابیر فنی وقعی ننهاده است. در آئین نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنتی رسا مصوب ۱۳۸۰ نیز در ماده ۵ استفاده از تدابیر فنی جهت تبادل اطلاعات در فضای سایبر را منوط به موافقت مرجع ثبت کننده اطلاعات نموده است. قانون گذار تنها استفاده از این تدابیر را جهت انتقال و مبادله اطلاعات در سیستم پیشنهاده داده و مشخص نیست که آیا یک شخص حقیقی یا حقوقی می‌تواند اطلاعات خود را در سیستم با استفاده از الگوریتم رمزنگاری ذخیره سازد حتی اگر قصد تبادل آن اطلاعات را نداشته باشد؟ اطلاعات به کار رفته در این مقرره نیز مطلق است و شامل هر گونه اطلاعاتی اعم از مالی و غیرمالی می‌شود. در این بند آمده به کارگیری هر گونه رمز برای تبادل اطلاعات مستلزم کسب موافقت مراجع مربوط و ثبت مشخصات، الگوریتم و کلید رمز مربوط و همچنین مشخصات متقاضی در دبیرخانه شورای عالی اطلاع رسانی یا مرجعی که معرفی می‌نماید، می‌باشد و در غیر این صورت ممنوع است. در سایر موارد این آئین نامه نیز به حفظ و حراست از حریم خصوصی اطلاعات و ارتباطات اشاره شده که بیشتر قانون گذار تدابیر واسطه‌ای را پیش بینی نموده و تنها اطلاعات خصوصی را ملحوظ نظر قرار داده است. در بند «ه» ماده ۱ آئین نامه استناد پذیری ادله الکترونیک مصوب ۱۳۹۳ آمده: برای حفاظت از داده‌ها باید زنجیره حفاظتی ایمن که امکان ردیابی داده‌ها را از مبداء تا مقصد فراهم می‌سازد، در نظر گرفت. در ماده ۳۸ این آئین نامه نیز به روش‌های توقیف داده‌ها پرداخته شده که اکثر راهکارهای ارائه شده در این مقرره تدابیر فنی اند. در این ماده واژه داده‌ها به طور مطلق استعمال شده و می‌تواند هم ناظر به اطلاعاتی که در مورد حریم خصوصی است و هم اطلاعات مالی باشد اما نکته قابل توجه این است که هر چند قانون گذار به استفاده از تدابیر فنی جهت حفاظت از مطلق اطلاعات پرداخته است اما این ماده ناظر به اطلاعاتی است که جنبه اثباتی دارند و قرار است به عنوان ادله

الکترونیک مورد استفاده قرار گیرند، به عبارت دیگر قانون گذار در این مقرره به استنادپذیری این اطلاعات به جهت داشتن ارزش اثباتی توجه نموده است و اقدام اش جنبه پسینی دارد و نه جنبه پیشینی. در قوانین موجود در حوزه فضای سایبر نیز به بحث حمایت از اطلاعات پرداخته شده است. برای نمونه در ماده ٤٠ قانون جرائم رایانه‌ای مصوب ۱۳۸۸ آمده: در توقیف داده‌ها با رعایت تناسب، نوع، اهمیت و نقش آن‌ها در ارتکاب جرم به روش هایی از قبیل چاپ، کپی برداری، غیرقابل دسترس کردن داده‌ها با روش هایی از قبیل تغییر گذر واژه یا رمزنگاری عمل می‌شود. واژه از قبیل نشان می‌دهد تدابیر فنی ذکر شده در این ماده حصری نیستند و تمثیلی اند و می‌توان از سایر تدابیر فنی نیز در توقیف داده‌ها استفاده کرد. تدابیر فنی پیش بینی شده در این ماده جهت حفظ و حراست از داده هایی مورد استفاده قرار می‌گیرند که در کشف یا اثبات جرایم به کار می‌روند از این رو استفاده از این تدابیر یک اقدام تمهیداتی قضایی یا اقدام چاره ساز است و نه یک تدبیر پیشگیرانه غیرکیفری که اختصاصا برای حفاظت از اطلاعات مالی پیش از ارتکاب جرم به کار رود. این تدابیر برای توقیف تمام داده‌ها صرف نظر از مالی یا غیرمالی بودن استفاده می‌شوند.

۳- جایگاه تدابیر فنی در اقدامات مراکز حامی امنیت فضای سایبر و پلیس فتا

مراکز بی شماری در عرصه فضای سایبر فعالیت می‌کنند که عملکرد این مراکز نیز بعدی پیشگیرانه دارد که از جمله آن‌ها می‌توان به مرکز ماهر[۱] و مرکز آپا[۲] اشاره کرد. مرکز ماهر مرکزی است که زیر نظر سازمان فناوری اطلاعات ایران جهت پاسخ گویی به رخدادهای امنیت کامپیوتر در سال ۱۳۸۵شکل گرفت. این مرکز اهداف مختلفی را در حوزه سایبری بر عهده گرفت که از جمله می‌توان به سیاست گذاری و توسعه و بهینه سازی روش‌های امنیتی، بررسی امکانات بالقوه ایجاد امنیت در فضای تبادل اطلاعات کشور و کمک به بالفعل نمودن این امکانات، کمک به تشکیل گروه‌های ضربت جهت حفاظت از امنیت اطلاعات و شبکه اشاره کرد. با تدقیق در اهداف یاد شده به نظر می‌رسد هر چند بخش عمده‌ای از وظایف این مرکز

۱- مرکز مدیریت امداد و هماهنگی عملیات رخداد
۲- مرکز آگاهی رسانه، پشتیبانی و امداد رایانه ای

تامین امنیت اطلاعات است با این حال تاکنون اقدامی فنی از سوی مرکز جهت حفاظت از مطلق اطلاعات صورت نگرفته است. این مرکز بیشتر تدابیر پیشگیرانه خود را در قالب تدابیر پیشگیرانه اجتماعی از جمله هشداردهی و آگاه سازی عمومی جهت حفاظت از اطلاعاتی که تنها مربوط به حریم خصوصی شهروندان است و افراد آن اطلاعات را در شبکه‌های اجتماعی خود بارگذاری نموده توجه داشته است و از توجه به وصف اطلاعات مالی و حتی هشدار در خصوص حفاظت از این اطلاعات غافل مانده است.

مرکز آپا نیز مرکزی است دانشگاهی که با هدف ارتقای آگاهی و درک مسائل مرتبط با امنیت اطلاعات در میان کاربران و سرویس دهندگان فضای سایبر از سال ۱۳۸٦ فعالیت خود را زیر نظر دانشگاه امیر کبیر آغاز کرد. این مرکز سعی دارد با ایجاد و استفاده از تکنولوژی مناسب امنیت اطلاعات را در مقابل حملات سایبری تامین سازد. این مرکز نیز همانند مرکز ماهر به شهروندان هشدارهایی برای حفاظت از اطلاعات شان در فضای سایبر می‌دهد اما این امر نافی اقدامات فنی این مرکز در حفاظت از مطلق اطلاعات نیست. دلیل این امر این است که این مرکز یک مرکز فنی مهندسی است و طبع اقدامات اش با تدابیر فنی سازگارتر است.

پلیس فتا[1] نیز که تنها نهاد پلیسی فعال در حوزه امنیت سایبری است اقدامات پیشگیرانه‌ای جهت حفاظت از اطلاعات مالی به عمل آورده است. این نهاد یک واحد تخصصی نیروی انتظامی است که در تاریخ ۳ بهمن ۱۳۸۹ به دستور فرمانده نیروی انتظامی جمهوری اسلامی ایران شروع به کار نمود. هدف اصلی تشکیل این پلیس مقابله با جرایم سایبری و حفاظت از اطلاعات بر روی شبکه اینترنت است. پلیس در این نهاد به دو قسم تقسیم می‌شود. نخست پلیس ستادی و دوم پلیس عملیاتی. پلیس‌های ستادی بنا به دستور مقام قضایی به رصد سایت-ها یا درگاه‌های الکترونیکی می‌پردازند و در صورت مجرمانه بودن محتوای این سایت‌ها یا صورت گرفتن یکی از جرایم مندرج در قانون در این فضا این امر را به مراجع قضایی اطلاع می‌دهند. این دسته از پلیس‌ها هر چند فی نفسه ماهیت کارشان پیشگیری از وقوع جرایم است و با گشت زنی در فضای سایبر تلاش می‌کنند شهروندان و یا مقامات قضایی را از تهدیدات موجود در این فضا آگاه کنند اما هیچ تدبیر فنی جهت حفاظت از اطلاعات مالی اتخاذ نکرده

۱- پلیس فضای تولید و تبادل اطلاعات ناجا

اند و تنها به هشداردهی و آگاه سازی عمومی از فواید و مضرات فضای سایبر بسنده کرده که بیشتر این هشدارها در خصوص حفظ حریم خصوصی است. دسته دوم پلیس‌های فتا، پلیس-های عملیاتی هستند که ماهیت عملکردشان اساسا پیگیری است و نه پیشگیری در معنای خاص. این گروه از پلیس‌ها بنا به دستور مقام قضایی در صورت تحقق یافتن جرم سعی در اعمال تدابیر واکنشی از جمله فیلتر نمودن سایت‌ها می‌کنند و اقدامات شان بیشتر واکنشی و در جهت پالایه محتوا است.

۴- اقسام تدابیر فنی حفاظت از اطلاعات در فضای سایبر

تدابیر پیشگیرانه فنی جهت حفاظت از اطلاعات مالی در فضای سایبر به چهار نوع تقسیم می‌شود: نخست تدابیر محدود کننده یا سلب کننده دسترسی، دوم تدابیر ناشناس کننده و رمزنگارها، سوم تدابیر صدور مجوز و چهارم تدابیر نظارتی. در تدابیر قسم نخست دسترسی به اطلاعات مالی برای اشخاص محدود یا اساسا غیرممکن می‌شود(انیسی حماسه،۱۳۸۹،۵۲). در تدابیر گروه دوم اطلاعات مالی تنها برای اشخاص مجاز رمزگشایی شده و با قرار دادن رمزهایی بر روی اطلاعات و یا استفاده از سایر شیوه‌های فنی، افراد غیرمجاز قادر به رمز گشایی اطلاعات نیستند و یا اطلاعات از تیررس آن‌ها پنهان باقی می‌ماند. در تدابیر قسم سوم سیستم تنها به افراد خاص مجوز دسترسی به اطلاعات را می‌دهد و در تدابیر قسم چهارم به افراد رخنه گر اجازه ورود به برخی وب سایت‌ها و درگاه‌های الکترونیک که در آن‌ها اطلاعات مالی ذخیره شده، داده نمی‌شود. در ادامه به تفصیل به تبیین این تدابیر پرداخته شده است.

۵-تدابیر محدود کننده یا سلب کننده دسترسی

این تدابیر در زمره مهم ترین تدابیر پیشگیرانه فنی هستند. در این تدابیر با نصب نرم افزارها یا سخت افزارهای خاص بر روی گره‌های دسترسی به شبکه از ورود یا ارسال برخی اطلاعات مالی برای افراد ناشناس جلوگیری یا دسترسی آن‌ها به این اطلاعات محدود می‌شود. هر چند برخی حملات سایبری حتی توسط به روزترین ضد بدافزارها تشخیص داده نمی‌شوند و دستیابی به امنیت صددرصدی موضوعی غیرعملی و محال است با این حال این موضوع قطعاً به معنای توقف استفاده از نرم‌افزارهای ضد بدافزار نیست؛ چرا که تولید چنین نرم‌افزارهایی

روز به روز هوشمندتر می‌شود و ممکن است نسخه‌های جدید آن‌ها قادر به تشخیص تهدیدات مختلفی باشند. در هر صورت استفاده از این نرم‌افزارها باعث می‌گردد حداقل دارنده متوجه شود که اطلاعات مالی موجود در سیستم رایانه اش دچار تهدید شده تا بتواند شروع به ترمیم خرابی و استفاده از پروتکل‌های بهبود نماید. از این رو برخی از شرکت‌هایی که دارای اطلاعات مالی بسیاری می‌باشند برای حفاظت بیشتر از داده‌های خود، با اتخاذ تدابیر حفاظتی اقدام به استخدام هکرهایی می‌نمایند تا با نفوذ به سیستم‌های رایانه‌ای شرکت، نقاط قوت و ضعف امنیتی سیستم‌های آنان را کشف کند(سیاری،۱۳۸۷،۱٤).

در صورتی که این تدابیر به طور مناسبی اجرا شوند تا حد قابل قبولی می‌تواند از افشای اطلاعات مالی ممانعت به عمل آورد. از مهم ترین مصادیق این دسته از تدابیر می‌توان به دفع آشغال، دیوار آتشین، سیستم تشخیص تجاوز، نرم افزارهای ضد پیام‌های ناخواسته، فیلترها و برنامه‌های ضداختلال اشاره نمود.

۵-۱- دفع آشغال

اطلاعات مالی آنلاین باید به نحو صحیح دفع شوند. منطقه‌ای که این اطلاعات بیشتر از دیگر مناطق در آن آسیب می‌پذیرند، حافظه اصلی سرورها است (angeline,George,Zachary,2003,22). اگر سیستم عامل قبل از محول کردن کاربر جدید به یک بلوک حافظه، اطلاعات کاربر را در کارت حافظه ذخیره سازد و آن‌ها پاک نکند، ممکن است کاربر جدید کلمات عبور، کلیدهای رمزی سازی و سایر اطلاعات مالی را که پشت برنامه قبلی ذخیره شده اند، بردارد. متأسفانه بسیاری از سیستم عامل‌ها چنین هستند و پاک کردن این اطلاعات را به عهده خود نرم افزار می گذارند.

۵-۲- باروی آتشین و انواع آن

ارتکاب بسیاری از جرایم رایانه‌ای در ابتدا نیازمند دسترسی غیرمجاز به اطلاعات مالی است. باروی آتشین یک دستگاه سخت افزاری یا یک برنامه نرم افزاری و یا ترکیبی از سخت افزار و نرم افزار است که دو عملیات اصلی را انجام می‌دهد. نخست جلوگیری از ورود اطلاعات ناخواسته مالی به رایانه و دوم جلوگیری از خروج اطلاعات ناخواسته مالی از رایانه(Gorman,2007,5).

وقتی مراکز ارائه کننده خدمات سطوحی از ارتباط را فراهم می‌آورند، این وظیفه باروی آتشین است که تضمین کند دسترسی اضافی به اطلاعات مالی خارج از محدوده تعریف شده مجاز نخواهد بود از این رو کار باروی آتشین کنترل ترافیک و دسترسی به اطلاعات مالی موجود در شبکه است. این بارو همانند دیواری بین رایانه و دنیای خارج عمل می‌کند و هر گونه ورود و خروج اطلاعات مالی را بین دنیای بیرون و داخل هماهنگ می‌کند. وجود یک باروی آتشین می‌تواند درصد بالایی از حملات سایبری علیه این اطلاعات را خنثی کند. با رشد روزافزون انواع برنامه‌های دانلود این امکان وجود دارد که یک برنامه جاسوسی[1] به همراه آن‌ها وارد رایانه شده و اقدام به جمع آوری و ارسال اطلاعات مالی افراد برای مقصدی نامعلوم نماید، در صورتی که یک باروی آتشین وجود داشته باشد این نرم افزار جاسوسی قادر نیست اطلاعات جمع آوری شده را ارسال نماید و حمله نیمه تمام می‌ماند(Solove,2003,15).

باروی آتشین به دو دسته تقسیم می‌شود، نخست باروی‌های آتشین سخت افزاری. این باروها دستگاه هایی هستند که معمولا برای حفاظت از اطلاعات مالی مجموعه‌ای از رایانه‌ها در مقابل نفوذ غیرمجاز و جاسوسی مورد استفاده قرار می‌گیرند. معمولا برای حفظ امنیت شبکه‌های رایانه‌ای باید از این باروها استفاده کرد. هر چه اطلاعات مالی یک شبکه رایانه‌ای مهم تر باشد، اهمیت استفاده از باروی‌های آتشین سخت افزاری قوی تر و البته گران تر بیشتر می‌شود. مثلا مجموعه شعب یک بانک تشکیل یک شبکه را می‌دهد که اطلاعات مالی آن بسیار مهم است و لذا باید از بهترین و قوی ترین باروی‌های آتشین برای جلوگیری از نفوذ هکرها استفاده کرد. از معروف ترین باروی‌های آتشین سخت افزاری می‌توان به باروی آتشین سخت افزاری سیسکو اشاره کرد. گروه دوم باروها باروی‌های نرم افزاری هستند. این باروها برنامه هایی هستند که به صورت نرم افزاری کلیه ورود و خروج اطلاعات مالی را به رایانه و یا از رایانه کنترل می‌کنند. این گونه باروی‌های آتشین مناسب استفاده‌های شخصی و خانگی و یا شبکه‌های کوچک مثل کافی نت‌ها می‌باشند(Wang,2006,11).

1-Spyware

۵-۳- سیستم تشخیص تجاوز[1]

این سیستم که دارای مرزهای مشترکی با سیستم قبلی (دیواره آتش) می‌باشد، نرم‌افزاری است که در صورت ورود غیرمجاز کاربر بیگانه به رایانه حامل اطلاعات مالی، به دارنده آن هشدارهای لازم را می‌دهد(موسوی مدنی،۱۳۸۵، ١٤). برای فهم بیشتر این سیستم می‌توان آن را در عالم واقع مشابه دزدگیرهایی دانست که برای ورود غیرمجاز طراحی شده‌اند، اما در عین حال بسته به نوع و مدل آن کارهای دیگری را نیز برای حفاظت از امنیت اطلاعات مالی انجام می‌دهد. به طور مثال می‌تواند مهاجمین به سیستم را به خود مشغول نموده و آن‌ها را از حمله به سیستم اصلی باز دارد.

۵-۴- نرم‌افزارهای ضد پیام‌های ناخواسته[2]

ارسال نامه‌های الکترونیکی با محتوای تجاری یا تبلیغاتی بدون اطلاع و رضایت دارندگان اطلاعات در بسیاری از مواقع موجب فریب و یا تحصیل اطلاعات مالی آن‌ها می‌گردد. هکرها از این روش به عنوان شیوه‌ای برای پخش ویروس نیز استفاده می‌نمایند، لذا ارائه‌کنندگان خدمات اینترنتی برای رفع این معضل استفاده از نرم‌افزارها و برنامه‌های ضد اسپم را توصیه می‌کنند.

۵-۵- فیلترها[3]

تدابیری هستند که از ورود یا ارسال برخی اطلاعات مالی جلوگیری می‌کنند. بعضی از آن‌ها عملکرد یک سویه دارند؛ یعنی از ورود اطلاعات مالی جلوگیری می‌نمایند و برخی کاربردی دو سویه داشته و علاوه بر ورودی‌ها، خروجی‌ها را نیز تحت کنترل قرار می‌دهند (باقری،۱۳۸۹،۳۲). فیلترکننده کلیه درخواست‌ها را با فهرست بانک اطلاعاتی خود که از سه جزء نشانی دامنه، نشانی پروتکل اینترنت و کلمه‌های کلیدی تشکیل شده مقایسه می‌نماید. اگر هیچ یک از این نشانی‌ها در فهرست درخواست رایانه وجود نداشته باشد، این درخواست

1- Intrusion Detection System(IDS)
2- Unsolicited Commercial Mail (UCM) or Spam
3- Filtering

نادیده گرفته می‌شود و در غیر این صورت، درخواست آلوده تشخیص داده شده و مسدود می-شود.

۵-۶- برنامه‌های ضداختلال

برنامه‌های ضداختلال برنامه هایی هستند که در برابر ویروس ها، کرم‌ها و تروا‌های رایانه‌ای سامان یافته اند(jay hoofnagle,2007,13). این برنامه‌ها شامل اقداماتی چون پویشگر ویروس[1]، پویشگر اکتشافی[2] و پویشگر کاربرد مرحله‌ای [3] هستند. پویشگر ویروس برنامه نرم افزاری است که برای بررسی و حذف ویروس رایانه ای، از بخش هایی از رایانه که در آن اطلاعات مالی ذخیره شده است، طراحی شده اند. پویشگر اکتشافی از تحلیل آماری، برای تعیین احتمال ویروسی بودن فایلی که در آن اطلاعات مالی نگهداری می‌شود، استفاده می‌کند. در این پویشگر از یک سیستم درجه بندی برای تعیین نوع ویروس‌ها استفاده می‌شود. پویشگر کاربرد مرحله‌ای به جای این که تمامی سیستم را محافظت کنند صرفا برخی بخش‌های خاص که ممکن است در آن اطلاعات مالی باشد را مورد پویش قرار می‌دهد. برای مثال خدمات پست الکترونیک راهی است که بسیاری از برنامه‌های مخرب از طریق آن وارد فایل اطلاعات مالی کاربران می‌شود. این پویشگر می‌تواند صرفا فایل‌های حاوی نامه‌های پست الکترونیک را به لحاظ وجود برنامه‌های مخرب مورد بررسی قرار دهد و از ورود آن‌ها به اطلاعات مالی جلوگیری کند.

۶- رمزنگارها

رمزنگارها ماهیت اصلی اطلاعات مالی را پنهان یا غیرقابل درک می‌کنند تا اطلاعات قابل شناسایی نباشد اما نباید از یاد برد که امکان استفاده از این برنامه برای مجرمان نیز وجود دارد، زیرا آن‌ها با رمزنگاری محتوای مجرمانه ارتباطات شان، امکان شناسایی خود را کاهش می-دهند(levy,2005,4**2**). از جمله این تدابیر می‌توان به رمزنگاری و سرّی نگاری اشاره کرد.

3- virus scanners
2- Heuristic scanners
5- Application – level virus scanners

۶-۱- رمزنگاری

یکی از ابزارهای دفاعی جهت حمایت از اطلاعات مالی استفاده از مکانیزم‌های رمزنگاری است. با رمزنگاری اطلاعات و فایل‌های باارزش می‌توان از جرایمی از قبیل دسترسی غیرمجاز به اطلاعات مالی جلوگیری نمود. رمزنگاری به عنوان بهترین راه حل جهت حفاظت از اطلاعات مالی شناخته شده است. مفهوم ساده رمزنگاری عبارت است از مبهم نمودن اطلاعات با استفاده از کلید رمزهای خاص به گونه‌ای که اطلاعات برای افراد غیرمجاز بی معنی و مبهم شوند و تنها فرد مجاز قادر به مشاهده و استفاده از این اطلاعات باشد(زیبر،۱۳۸۳،۲۱). فن آوری رمزنگاری روشی است که جهت ممانعت از دسترسی غیرمجاز دیگران به اطلاعات مالی افراد مورد استفاده قرار می‌گیرد و در برابر حملات خصوصاً شنود اطلاعات بسیار کارایی دارد. با استفاده از رمزنگاری می‌توان سه سرویس امنیتی را ارائه کرد: محرمانه سازی اطلاعات به این معنی که از افشاء اطلاعات مالی برای اشخاصی که صلاحیت دسترسی به آن‌ها را ندارند، خودداری می‌شود، حفظ تمامیت اطلاعات مالی به این معنی که اطلاعات اصالت خود را حفظ نموده و در معرض تغییر، محو و هک قرار نمی‌گیرند و مجوزسنجی اطلاعات مالی یعنی حفظ منشاء این اطلاعات و جلوگیری از تکذیب اطلاعاتی که از منشاء آمده اند. رمزنگاری قدمتی بسیار طولانی دارد و کشورها در طول تاریخ و خصوصاً در زمان جنگ‌ها برای محرمانه ماندن اطلاعات مهم شان از آن استفاده می‌نمودند(ابوالحسن پور،۱۳۸٦،۲۰).

رمزنگاری برای اطلاعات مالی سایبری، حکم قفل برای اطلاعات چاپی را دارد. اطلاعات به وسیله درهم سازی به نحوی که فقط با یک کلید محرمانه از حالت درهم خارج شود، مورد حفاظت قرار می‌گیرند. پیام درهم ریخته شده که «متن سرّی[1]» نامیده می‌شود، پیام هایی که باید رمزنگاری شوند «متن ساده[2]» نام دارند، اما متن خروجی فرآیند رمزنگاری را «متن رمزی[3]» می‌نامند. رمزنگاری روش‌های متفاوتی دارد؛ از این روش‌ها می‌توان به روش‌های جایگزینی، جابجاسازی (پس و پیش کردن)، پنهان سازی، سیستم ابزاری و الگوریتم‌های ریاضی با کدهای منبع اشاره کرد. اغلب رمزها با دو نوع اصلی دگرگونی شکل، یعنی با «جایگشت» و «جانشینی»

1- ciphertext
2- Plain text
3- Chipper text

تشکیل می‌شوند. در جایگشت، ترتیب قرار گرفتن کاراکترها یا «بیت ها» تغییر می‌کند؛ در حالی که در جانشینی، بیت ها، کاراکترها یا بلوک‌ها تغییر می‌کنند و بیت ها، کاراکترها یا بلوک‌های دیگری جانشین آن‌ها می‌شوند. برای «رمزگشایی» شخص باید هم به روش و هم به کلیدی که رمزی سازی با آن انجام شده، آگاهی داشته باشد (japkoops,2005,21). برخلاف روش‌های رمزنگاری که ثابت اند و همه از الگوریتم آن مطلع اند، رمز این الگوریتم‌ها متغیر است و تنها با یک کلید محرمانه کار می‌کند که آن کلید برای فردی که صاحب اطلاعات می‌باشد قابل کدگشایی است.

سیستم‌های رمزنگاری به دو نوع رمزنگاری متقارن و رمزنگاری نامتقارن تقسیم می‌شوند. در رمزنگاری متقارن[1] یا کلید خصوصی برای رمزنگاری و رمزگشایی از یک کلید استفاده می‌شود، این روش رمزنگاری به روش تک کلید معروف است. در این رمزنگاری هر یک از رایانه‌ها دارای یک کلید محرمانه بوده که این کلید بسته‌های اطلاعاتی را رمزگشایی می‌کند. در روش فوق می‌بایست ابتدا نسبت به اطلاعات مالی که در بستر سامانه‌های رایانه‌ای و مخابراتی ذخیره شده اند آگاهی کامل وجود داشته باشد. هر یک از رایانه‌های شرکت کننده در مبادله اطلاعاتی می‌بایست دارای کلید رمز مشابه به منظور رمزگشایی اطلاعات باشند. برای رمزنگاری اطلاعات ارسالی نیز از کلید فوق استفاده خواهد شد(romanosky,2012,17).

رمزنگاری نامتقارن[2] یا کلید عمومی در ابتدا با هدف مشکل انتقال کلید در رمزنگاری متقارن پیشنهاد شد. در رمزنگاری نامتقارن یا عمومی از ترکیب یک کلید عمومی و یک کلید خصوصی استفاده می‌شود. در این سیستم هر شخص یک جفت کلید دریافت می‌کند که یکی کلید عمومی نام دارد و دیگری کلید اختصاصی. کلید عمومی برای اطلاع عموم منتشر می‌شود ولی کلید اختصاصی محرمانه نگه داشته می‌شود. به این ترتیب دیگر نیازی نیست که فرستنده و گیرنده از یک کلید محرمانه مشترک استفاده کنند، بلکه تمام ارتباطات از طریق کلید عمومی انجام می‌شود و نیازی به ارسال کلید اختصاصی نیست(Swire,2012,480). در این سیستم احتیاجی به برقراری یک کانال ارتباطی مطمئن نیست، بلکه تنها لازم است که کلیدها به روش

1- Symmetric Encryption (or private Key)
2- Asymmetric Encryption (or Public Key)

مطمئنی به کاربرها اختصاص یابند. هر دو کلید با استفاده از عملیات ریاضی بر روی اعداد اول تهیه شده‌اند و با یکدیگر مرتبط هستند به گونه‌ای که رابطه‌ی رمزنگاری شده با هر یک از کلیدها، قابل رمزگشایی با کلید دیگری می‌باشد(Govinda,2011,2).

۶-۲- سرّی نگاری

سرّی نگاری، نوعی مخفی کردن اطلاعات مالی است بدون آن که اصل اطلاعات دچار تغییر گردد. این کار با قرار دادن اطلاعات در داخل یک سند، تصویر، نوار صوتی یا ویدیوئی انجام می‌گیرد. هر کس که بداند آن واسط، حاوی اطلاعات با ارزشی است، اگر روش رمز گذاشتن را بداند می‌تواند اطلاعات را استخراج کند ولی آن پیام، برای دیگری کاملاً نامرئی است(mason,2006,34).

سرّی نگاری دارای روش‌های متنوعی است از جمله این روش‌ها می‌توان به ریز نقطه و قرار دادن اطلاعات در داخل تصویر دیجیتال[1] اشاره کرد. ریز نقطه، صفحاتی آنلاین به اندازه یک نقطه است که یک صفحه کامل اطلاعات را به وضوح تمام نشان می‌دهد(فیروزمش،۱۵،۱۳۸۸). برای مخفی کردن اطلاعات در فایل‌های تصویری و صوتی علاوه بر ریز نقطه ابزارهای متعددی دیگری نیز وجود دارد برای نمونه با اس – تولز[2] می‌توان اطلاعات مالی را به سادگی با کشاندن نماد تصویری بر روی تصویر، در تصویر پنهان کرد. اگر امنیت بیشتری مورد نظر باشد، می‌توان اطلاعات را نخست رمزی سازی نمود و سپس در درون یک تصویر با استفاده از رمز دیگری جاساز نمود. از سرّی نگاری می‌توان برای پنهان کردن اطلاعات مالی در دیسک سخت رایانه نیز استفاده کرد.

۷- تدابیر صدور مجوز

در این تدابیر تنها به افرادی اجازه ورود به پایگاه اطلاعات مالی داده می‌شود که تائیدیه داشته باشند. تائیدیه در صورتی صادر می‌شود که فرد توسط سیستم شناسایی شود در این روش این امکان فراهم می‌شود که رایانه حاوی اطلاعات بداند که کاربر کیست و سپس به او مجوز

1- Microdots
2- S-Tools

بدهد. این اقدام می‌تواند از ورود افرادی که صلاحیت لازم جهت دسترسی به اطلاعات مالی را ندارند، جلوگیری نماید و تنها به افرادی اجازه عبور دهد که نسبت به هویت و اعمال آن‌ها اطمینان وجود دارد(kerr,2005,60). برای صدور مجوز یا تصدیق هویت کاربر می‌توان از سیستم‌های شناسایی متنوعی کمک گرفت که از جمله می‌توان به امضای دیجیتال، گواهی‌های رقومی، شناسایی دو عاملی، توکن و بیومتریک اشاره کرد.

۷-۱- امضای دیجیتال

امضای دیجیتالی، بلوکی از داده است که به اطلاعات مالی پیوست می‌شود و آن اطلاعات را به شخص یا موسسه خاصی منسوب می‌کند. این پیوند به نحوی است که امضاء می‌تواند توسط دریافت کننده اطلاعات یا شخص ثالث مستقل تأیید شود و نمی‌توان آن را جعل کرد. اگر حتی یک بیت از اطلاعات مالی حذف شده باشد، امضاء در فرآیند تأمین اعتبار رد می‌شود. امضاء دیجیتالی اعتبار منبع اطلاعات مالی را نشان می‌دهد(gaur,2015,22).

این فناوری با استفاده از تکنولوژی مطمئنی نظیر زیرساختار کلید عمومی، ایجاد می‌شود و معمولاً اطلاعات مالی را به یک سند الکترونیکی ضمیمه می‌سازد و از تولید کننده یا ذخیره کننده و یا پردازش کننده آن اطلاعات می‌خواهد که امضای دیجیتالی خود را به آن ضمیمه سازد تا امکان انکار آن اطلاعات از بین رود و هویت کسی که امضاء به او منتسب می‌شود معلوم گردد(Greenleaf,1997,11).

اولین مرحله برای به کار بردن امضای دیجیتالی این است که یک جفت کلید عمومی و خصوصی ایجاد شود. کلید خصوصی توسط فرستنده اطلاعات به صورت محرمانه نگهداری می‌شود و کلید عمومی به صورت آنلاین در دسترس قرار می‌گیرد. دومین مرحله این است که فرستنده با ایجاد کردن یک خلاصه منحصر به فرد از اطلاعات مالی چکیده آن اطلاعات و رمزگذاری شان را به صورت دیجیتالی تأیید و امضاء می‌نماید. فرستنده متن اصلی اطلاعات را با استفاده از یک فرمول ریاضی خاص، به یک پیام فشرده تبدیل می‌کند که به آن «نتیجه خرد» گفته می‌شود. نتیجه خرد برای اصل هر اطلاعاتی منحصر به فرد است. در واقع نسبت «نتیجه خرد» به اصل اطلاعات، مانند نسبت اثر انگشت، برای انسان است. سومین مرحله این است که پیام را امضای دیجیتالی نماید و سپس آن را برای گیرنده بفرستد. در این مرحله «نتیجه خرد» به

وسیله کلید خصوصی اصل ساز (منشا اصلی داده پیام) رمزگذاری می‌شود و به اطلاعات اصلی ضمیمه می‌گردد سپس پیامی که امضاء دیجیتال ضمیمه آن شده به وسیله کلید عمومی مخاطب رمزگذاری می‌شود و برای مخاطب ارسال می‌شود. چهارمین مرحله مخاطب پس از دریافت پیام، ابتدا آن را به وسیله کلید خصوصی خودش رمزگشایی می‌کند آنگاه امضاء دیجیتالی را به وسیله کلید عمومی ارسال کننده رمزگشایی می‌کند و به نتیجه خرد دست می‌یابد و نهایتاً، مخاطب یک پیام فشرده دیگری از پیام اصلی ایجاد و آن را با پیام رمزگذاری شده مقایسه می‌کند، اگر آن دو نتیجه خرد (پیام فشرده) با هم مطابقت داشتند، گیرنده پی می‌برد که پیام تغییر نیافته است(chawki,2005,27).

با امضای دیجیتال چهار اصل امنیت اطلاعات مالی تضمین می‌شود: نخست تأیید هویت، گیرنده می‌تواند مطمئن باشد که فرستنده کیست. دوم تمامیت، گیرنده می‌تواند مطمئن باشد که اطلاعات مالی حین انتقال تغییر پیدا نکرده است. سوم انکارناپذیری، فرستنده نمی‌تواند امضای اطلاعات مالی را انکار کند. چهارم محرمانگی، گیرنده می‌تواند مطمئن باشد که اطلاعات مالی جزء او برای سایرین افشاء نشده اند. برخلاف کلیدهای مورد استفاده در رمزی سازی(محافظت از محرمانه بودن اطلاعات مالی)، کلیدهای خصوصی مورد استفاده برای امضاء کردن اطلاعات مالی فشرده معمولاً به منظور بازیافت کلید بایگانی نمی‌شود. اگر کلید خصوصی یک امضاء گم شود، می‌توان یک کلید نو ساخت و کلید عمومی قدیمی را منقضی کرد(احمدی،۱۳۸۸،۲۷).

۷-۲- گواهی‌های رقومی

گواهی‌های رقومی، گواهی هایی هستند که به حل مسئله ایمنی اطلاعات مالی در فضای سایبر کمک می‌کند. این گواهی‌ها از سوی متصدیان درگاه‌های الکترونیکی مورد استفاده قرار می‌گیرند(احسانی موید،۱۳۸۹،۱۶). این متصدیان موسسات تجاری هستند که هویت افراد یا سازمان‌های دارای اطلاعات مالی را در وب تأئید و تأئیدیه هایی مبنی بر درستی هویت شان صادر می‌کنند. برای صدور یک گواهی، ممکن است از فرد خواسته شود که یک کارت شناسایی (مانند کارت رانندگی) را نشان دهد. گواهی‌های رقومی، یک شبکه امن برای حفاظت از اطلاعات مالی ایجاد می‌کنند(Jay hoofnagle,2007,18).

۷-۳- شناسایی دو عاملی[1]

این راهبرد فنی برای بررسی مجاز بودن کاربر در دسترسی به اطلاعات مالی از دو عامل استفاده می‌کند. ایده به وجود آمدن این تدبیر امنیتی از آن جا ناشی می‌شود که هر چه تعداد عوامل شناسایی مجزا بیشتر باشد، عملیات قابل اعتمادتر و در نتیجه دارای خطر کمتر خواهد بود. فهم این مدل شناسایی بسیار ساده است، در این روش سیستم برای دسترسی به اطلاعات مالی تنها به یک عامل (مثلا رمز عبور) اکتفا نکرده و از عامل و یا فاکتور دوم برای شناسایی فرد استفاده می‌کند. به عنوان مثال کارت مخصوص خودپردازهای بانکی را در نظر بگیرید یک مشتری بانک برای انجام عملیات بانکی به یک کارت و یک رمز عبور نیازدارد. دستگاه خودپرداز به کاربری که فقط یکی از این عوامل را داشته باشد پاسخ نخواهد داد و کار با دستگاه ATM مستلزم داشتن هر دو عامل از طرف کاربر است. می‌توان دریافت که هر ترکیب دوتایی از موارد فوق می‌تواند یک ترکیب کاملاً مناسب برای شناسایی دو عاملی کاربر در نظر گرفته شود(jayhoofnagle,2010,2). به عنوان مثال ترکیب یک شماره شناسایی شخصی به همراه یک توکن امنیتی می‌تواند یک شناسایی دو عاملی نسبتاً مناسب را ایجاد کند. شخص با داشتن این دو عامل می‌تواند اطلاعات مالی خود را را بروزرسانی کند بدون این که نگران امنیت اطلاعات مالی خود باشد. این ابزار شناسایی تا حد زیادی از سرقت اطلاعات مالی و تخریب و هک آن‌ها جلوگیری می‌کند.

۷-۴- توکن

توکن به معنی سخت افزاری است که از آن برای حفاظت از اطلاعات مالی در محیط‌های سایبری استفاده می‌شود (Gorman,2007,12). توکن یک قطعه سخت افزاری یا نرم افزاری است که توسط کاربر رایانه اجرا می‌شود یا در اختیار او می‌باشد. توکن حاوی گذرواژه‌ای است که به صورت الکترونیکی ثبت و رمزنگاری شده است. علاوه بر آن توکن دارای پردازنده‌ای است که در مواقع لزوم، می‌تواند گذرواژه‌ها را ذخیره یا بازیابی کند. این راهبرد امنیتی یک ابزار الکترونیکی است که عمل اثبات هویت فرد صاحب اطلاعات مالی را به صورت الکترونیکی و

1- TwoFactorAuthentication

از طریق راهکار شناسایی دوعاملی یا چند عاملی انجام می‌دهد. در حقیقت توکن امنیتی یک کلید الکترونیکی قدرتمند برای ورود به پایگاه‌های اطلاعات مالی است. توکن ها، با دارا بودن حافظه داخلی و بهره گیری از پردازنده‌ای قدرتمند می‌توانند به رایانه متصل شده و از طریق نرم افزار مخصوص، عملیات رمزنگاری و تشخیص هویت افراد را اجرا کنند. توکن‌های پرکاربرد امروزی معمولاً مجهز به پورت USB بوده و می‌توانند عمل تبادل اطلاعات مالی را با سرعت بالا و به نحوی که برای کاربر بسیار ساده باشد انجام دهند. بعضی از توکن‌ها کلیدهای رمزنگاری مانند امضای دیجیتال و اطلاعات بیومتریک مثل اثرانگشت را در حافظه خود ذخیره می‌کنند(عبدالله خانی،۱۳۸٦،۱٤). این توکن‌ها شامل چند کلید برای وارد کردن شماره شخصی شناسایی فرد صاحب اطلاعات و آغاز برنامه توکن برای انجام عملیات ایجاد رمزعبور است. وقتی توکن به دستگاه رایانه وصل می‌شود، فرد تنها با وارد کردن شناسه امنیتی مخصوص به خود می‌تواند وارد سیستم شده و به اطلاعات مالی انباشته شده در آن سیستم دسترسی داشته باشد(ساجدی،۱۳۸٦،۱۳). توکن‌ها دارای انواع مختلفی هستند، گروهی از توکن‌ها هیچ اتصال فیزیکی با رایانه ندارند و تنها در درون خود یک صفحه نمایش دارند که اطلاعات مالی کاربر تنها در درون آن نمایش داده می‌شود. این توکن‌ها برای حمایت از اطلاعات مالی برخط مورد استفاده قرار می‌گیرند که از آن به توکن‌های غیرمتصل تعبیر می‌شود. گروه دیگری از توکن‌ها توکن‌های متصل اند. این توکن‌ها باید حتما به صورت فیزیکی به رایانه شخصی متصل شوند، این اتصال باعث می‌شود اطلاعات مالی اشخاص به رایانه شخصی منتقل شود. برای برقراری ارتباط در این نوع از توکن‌ها باید از کارت‌های ورود هوشمند و USB استفاده شود(Hoffman,2008,11).

۷-۵- بیومتریک

بیومتریک در اصطلاح به هر خصوصیت فیزیولوژیکی یا رفتاری منحصر به فرد، متمایز کننده، مقاوم و قابل سنجش اطلاق می‌شود که بتواند برای تعیین یا تایید خودکار هویت فرد صاحب اطلاعات مالی و به تبع حفظ اطلاعات اش به کار رود. بیومتریک بر دو قسم است نخست خصوصیات فیزیولوژیکی، که به ساختار و شکل بدن مربوط می‌شوند. برای نمونه می‌توان به شناسایی از طریق اثر انگشت، نقشه کف دست، نقشه رگ‌های دست، صوت، عنبیه نگاری،

شبکیه نگاری، چهره نگاری، شکل گوش، بوی بدن، ساختار ناخن، صوت و هندسه دست اشاره کرد. دوم خصوصیات رفتاری، این قسم از بیومتریک برخی از رفتارهای انسان را مورد واکاوی قرار می‌دهد برای نمونه امضاء، چگونگی راه رفتن، تشخیص لبخند و نحوه تایپ نمونه‌ای از این شیوه اند(هاتف،۱۳۸٦،۷۵).

۸- تدابیر نظارتی

در تدابیر پیشگیرانه مربوط به نظارت بر ورودی‌ها سعی می‌شود از دسترسی اشخاص نفوذگر به اطلاعات مالی جلوگیری شود. این نظارت اهمیت فراوانی در حفاظت از اطلاعات مالی دارد و حفاظت دقیقی از این اطلاعات به عمل می‌آورد به گونه‌ای که حتی بسیاری از سامانه‌های نظارتی اطلاعات مربوط به تلاش‌های موفق یا ناموفق افراد در ورود به بخش هایی که در آن اطلاعات مالی ذخیره شده است را ثبت می‌کنند(اسدی،۱۳۸٤، ۱۵). کنترل ورودی‌ها کمک می‌کند از میزان اطلاعات مالی وارد شده، نوع و منشاء آن‌ها به ویژه در حالت هایی که به دلیل بالا بودن هزینه امکان به کارگیری کنترل‌های دولایه و تکنیک‌های تهیه مجوز وجود ندارد، اطمینان حاصل نمود(یزدانی زنور،۱۷،۱۳۸۷). راه‌های گوناگونی برای کنترل ورودی‌ها وجود دارد که ساده ترین آن استفاده از رمزعبور در رایانه است(عباسی،۲۲،۱۳۸۹). بدیهی است که بالا بردن ضریب کنترل می‌تواند به مثابه مانعی در برابر مجرمان باانگیزه عمل کند و آن‌ها را در دستیابی به آماج جرم ناکام بگذارد.

از دیگر راهکارهایی که می‌تواند به عنوان کنترل ورودی عمل کند استفاده از شبکه‌های مجازی کاوشگر الکترونیک است. این کاوشگرها که از آن‌ها به پلیس مجازی تعبیر می‌شود وظیفه کنترل دسترسی به اطلاعات مالی را بر عهده دارند. علاوه بر نظارت ورودی نظارت بر خروجی نیز اهمیت شایانی دارد و مکمل کنترل ورودی است. در این نوع نظارت علاوه بر این که تمامی راه‌های خروج اطلاعات مدنظر قرار می‌گیرد به احتمال نشت اطلاعات مالی در فضای سایبر نیز توجه می‌شود. در این سیستم کنترلی تمام اطلاعات مالی که منشأ خود را ترک می‌کنند مورد بررسی و نظارت کامل قرار می‌گیرند. این نظارت به دو شکل هم‌زمان و غیرهم-زمان صورت می‌گیرد. در حالت نظارت هم‌زمان، ابزار الکترونیکی، مسئول یا متصدی مربوطه را

از فعالیت غیرمجاز شخص در دسترسی به اطلاعات مالی در همان زمان آگاه می‌کند و به این ترتیب او می‌تواند اقدامات پیشگیرانه مقتضی را انجام دهد؛ اما در حالت نظارت غیرهم‌زمان، بسته به میزان دقت ابزار نظارتی، صرفاً بخش‌های گزینش شده‌ای از فعالیت‌های این اشخاص ثبت می‌شود تا در فرصتی دیگر با بررسی آن‌ها موارد غیرمجاز دسترسی اشخاص به اطلاعات مالی مشخص گردد. در این حالت ابزارها و برنامه‌هایی بر روی سیستم شخص نصب می‌شود که کلیه فعالیت‌های شبکه‌ای اش حتی ضرباتی که بر روی صفحه کلیدش زده یا نقاطی که به وسیله موس بر روی آن‌ها کلیک کرده، ضبط می‌گردد(جلالی فراهانی،۱۳۸۸،۱۱۱). در این کنترل، تمامی راهکارهای نظارتی در مورد خروج اطلاعات مالی مدنظر قرار می‌گیرد و تمامی اطلاعات مالی ذخیره شده دارای کدبندی مشخصی می‌شوند و بدین ترتیب از تمامیت آن‌ها حفاظت می‌شود.

نتیجه گیری

با توجه به مطالب ارائه شده به نظر می‌رسد اطلاعات مالی جوهره فضای سایبر است که به هر دستاویزی از سوی افراد سودجو مورد حمله قرار می‌گیرد. این اطلاعات بنیان فضای سایبری به شمار می‌رود و همه اموالی که در فضای واقعی هستند، در قالب این اطلاعات در فضای سایبر پدیدار شده اند از این رو با توجه به تغییر ماهیت اموال از سنتی به سایبری دیگر نمی‌توان به شیوه‌های فیزیکی جهت حفاظت از اموال خوشبین بود بلکه باید بیشتر از تدابیری استفاده نمود که از جنس همین فضا و دارای ویژگی‌های آن باشند که این تدابیر چیزی جزء تدابیر نظارت فنی که مقید به وسیله است، نمی‌باشد. در این تدابیر با به کارگیری برنامه‌ها و راهبردهای تخصصی و فنی از اطلاعات مالی حفاظت می‌شود. این تدابیر بیشتر ناظر به حفاظت از بستر ورود اطلاعات مالی(ورودی ها) و بستر خروج اطلاعات مالی(خروجی ها) است تا در پرتو این نظارت از رفتارهای مخاطره آمیزی که در فضای مابین ورودی‌ها و خروجی‌ها علیه این اطلاعات صورت می‌گیرد، پیشگیری کند. بهترین برنامه این تدابیر، برنامه محدود کننده یا سلب کننده دسترسی به اطلاعات مالی است چرا که این برنامه منطبق با هدف پیشگیری وضعی است. در مصوبات موجود در حوزه فضای سایبری و قوانین موجود در این راستا نیز قانون گذار گاه به طور ضمنی و گاه به طور صریح به استفاده از این تدابیر جهت تامین امنیت فضای سایبر پرداخته که با تدقیق در تعابیر استفاده شده در متون قانونی سه نکته قابل استنباط است؛ نخست این که مقنن تنها به تامین امنیت شبکه و حفاظت از اطلاعاتی که مربوط به حریم خصوصی شهروندان است پرداخته و توجهی به اطلاعات مالی نداشته است، دوم این که به همه شیوه‌های فنی توجهی ننموده و صرفا به شیوه هایی چون باروی آتشین پرداخته است و سوم اقدامات وی بیشتر در جهت پالایش محتوا است و رویکرد حفاظتی ندارد. از مراکز فعال در حوزه امنیت سایبر تنها ماهیت اقدامات آپا، فنی است آن هم تنها جهت حفاظت از اطلاعات شخصی کاربران که در شبکه‌های اجتماعی بارگذاری شده اند، از این تدابیر استفاده می‌کند. پلیس اداری فتا نیز نسبت به اعمال تدابیر پیشگیرانه فنی جهت حفاظت از هر گونه اطلاعاتی در فضای سایبر بیگانه است و تنها با آگاه سازی شهروندان از تهدیدات این فضا از خود کاربران می‌خواهد که از تدابیر امنیتی جهت حفاظت از اطلاعات شان استفاده کنند، از این رو این نهاد پلیسی نیز اساسا با وصف اطلاعات مالی آشنا نیست و بیشتر اقدامات ش پسینی و ناظر بر فیلترینگ است.

منابع

- ابوالحسن پور، وحیده، ۱۳۸٦، شبکه‌های مجازی اختصاصی، **مجله الکترونیکی پژوهشگاه اطلاعات و مدارک ایران**، دوره ۵، شماره ۲، ص ۲۰ -۱.
- احسانی مؤید، فرزانه، ۱۳۸۹، ورود جاسوس‌ها ممنوع، **ماهنامه اطلاعات**، سال یازدهم، شماره ۱۲، ص ۱۸ - ۱.
- احمدی، جواد، ۱۳۸۸، دنیای بیومتریک، **ماهنامه فناوری**، سال چهارم، شماره ۱۳، ص ۲۸-۱۳.
- اسدی، مریم، ۱۳۸٤، فناوری‌های امنیت اطلاعات: با یک دیدگاه طبقه بندی، **فصلنامه علوم اطلاع رسانی**، دوره ۲۰، شماره ۳ و ٤، ص ١٦-۱.
- انیسی حماسه، زهره، ۱۳۸۹، امضای دیجیتال راهکاری مؤثر در پیشگیری از جرایم رایانه ای، **مجله عصر فناوری اطلاعات**، سال ششم، شماره ٥٦، ص ۵۳ - ٤٨.
- باقری، فاطمه، ۱۳۸۹، مکانیزم‌های تصدیق هویت در برابر سرقت اطلاعات، **مجله عصر فناوری اطلاعات**، شماره ۵۳، ص۵۳ -۲۷.
- جاویدنیا، جواد، ۱۳۸۸، **جرایم تجارت الکترونیک**، تهران، انتشارات خرسندی، چاپ دوم.
- جلالی فراهانی، امیرحسین، ۱۳۸۸، نهادسازی برای پیشگیری از جرایم سایبری با نگاهی به قانون جرایم رایانه‌ای، در رویکرد چند نهادی به پیشگیری از جرم، **مجموعه مقاله‌های ملی پیشگیری از وقوع جرم**، چاپ اول، معاونت آموزش و پیشگیری از ناجا، تهران، ص ۵-۳۰.
- جوان جعفری، عبدالرضا، ۱۳۸۹، جرایم سایبر و رویکرد افتراقی حقوق کیفری، **مجله دانش و توسعه**، سال هجدهم، شماره٣٤، ص۲۳-۱.
- حسن بیگی، ابراهیم، ۱۳۸٤، **حقوق و امنیت در فضای سایبر**، چاپ اول، تهران، انتشارات مؤسسه مطالعات و تحقیقات بین المللی ابرار معاصر تهران.
- خانعلی پور، سکینه، ۱۳۹۰، **پیشگیری فنی از جرم**، چاپ اول، تهران، انتشارات میزان.

– خالقی پوستچی، علی، ۱۳۸۸، پیشگیری از جرایم سایبر با بهره‌گیری از فناوری اطلاعات و ارتباطات (ICT) ، **مجموعه مقاله‌های همایش ملی علمی کاربردی پیشگیری از جرم**، چاپ اول، انتشارات میزان .

– زیبر، اولریش، ۱۳۸۳، **جرایم رایانه ای**، مترجم: محمدعلی نوری، رضا نخجوانی، مصطفی بختیاروند، احمد رحیمی مقدم، چاپ اول، تهران، انتشارات گنج دانش.

– سیاری، هومن، ۱۳۸۷، باروی آتشین چیست، **مجله رایانه خبر**، سال نهم، شماره ۷ ۵، ص۳۵-۱۰.

– ساجدی، حامد، ۱۳۸٦، بیومتریک، فناوری در خدمت امنیت، **مجله تکفا**، سال پنجم، شماره ۷، ص ۱٤۲- ۱۳٤.

– صفاری ، علی، ۱۳۸۰، مبانی پیشگیری از وقوع جرم، **فصلنامه تحقیقات حقوقی**، شماره ۳۳و۳٤، ص۲۹-۱.

– عالی‌پور، حسن، ۱۳۹۰، **حقوق کیفری فناوری اطلاعات**، چاپ اول، تهران، انتشارات خرسندی.

– عباسی، مراد، ۱۳۸۹، حریم خصوصی، فضای مجازی و چالش‌های پیشگیرانه فراروی ناجا، **فصلنامه مطالعات پیشگیری از جرم**، سال پنجم، شماره ۱۷، ص۲۷-۵.

– عبدالله خانی، علی، ۱۳۸٦، **جنگ نرم ۳(نبرد در عصر اطلاعات)**، چاپ اول، تهران، انتشارات موسسه فرهنگی مطالعات و تحقیقات بین المللی ابرار معاصر ایران.

– فیروزمنش، افشین، ۱۳۸۸، امنیت و حریم خصوصی در فضای مجازی، **گاهنامه تحلیلگران عصر اطلاعات**، سال چهارم، شماره ۳۰، ص۱۵-۷.

– فضلی، مهدی، ۱۳۸۹، **مسئولیت کیفری در فضای سایبر**، چاپ اول، تهران، انتشارات خرسندی.

– موسوی مدنی، فریبرز، ۱۳۸۵، حفاظت از حریم شخصی و امنیت اطلاعات کاربران وب سایت ها، **مجله فناوری اطلاعات**، شماره ۱۰، ص۲۷-۱۰.

- هاتف، مهدی، ۱۳۸٦، بیومتریک رویکردی نوین در تأمین امنیت، **دوماهنامه توسعه انسانی پلیس**، سال چهارم، شماره ۱۲، ص ۸٤ - ۷۰.
- یزدانی زنور، هرمز، ۱۳۸۷، حریم خصوصی در فضای سایبر، **مجله حقوق فناوری اطلاعات و ارتباطات**، شماره ۲۷، صص۱۹-۵.
- قانون جرائم رایانه‌ای مصوب ۱۳۸۸
- آئین نامه واحدهای ارائه کننده خدمات اطلاع رسانی و اینترنتی رسا مصوب ۱۳۸۰
- آیین نامه استناد پذیری ادله الکترونیک مصوب ۱۳۹۳
- Chawki, Mohamad; AbdelWahab, Mohamad, 2005, Identity **Theft in Cyber Space: Issues and Solution**, George Town University Law Center, Vol.3.
- Gaur, Priyanka; Srivastava, Prabhat, 2015, **Biometric Risks - How to Deal with the Challenges**, Scholedge International Journal of Management & Development, Vol. 2, No.7.
- Greenleaf, Graham; Clarke, Roger, 1997, **Privacy Implications of Digital Signatures**, IBC Conference on Digital Signatures (Proc.), Sydney, pp. 1 - 12.
- Gorman, Sandra, 2007 ,**securing business front door,password,token and biometric**, No. 03-07,pp.1-27.
-Hoffman, sandrak, 2008, **Mcginiey,trancy.Identitytheft**, publishing by group greenwood, No.2, pp.7-17.
- Jay hoofnagle, chris, 2007, **Big brothers little helpers:howchoicepoint and other commercial data brokers collect package your data for law enforcement**, publishing by group greenwood, 29 n. c. j. intll and com. Reg,No.2,pp.13-35.
- Jay hoofnagle, chirs, 2010, **Identity theft:making the know un knows know**,vol. 21,No.1.
- K.Govinda; E.Sathiyamoorth, 2011, **Multilevel Cryptography Technique Using Graceful Codes**, Journal of Global Research in Computer Science, Vol. 2, No. 7, pp. 1-5.
- Kerr, Orins, 2005, **Digital Evidence And the New Criminal Procedure**, The George Washington University Law School Public Law and Legal Theory Working Papper, No. 108, pp. 1-62.

- Levy. S, Grand, 2005, **Theft Identity**, The American Journal of International Law, Vol. 80, No. 1, pp. 40-60.
- Mason, Stephan, 2006, **Electronic Signature in Practice**, Journal of High Technology Law, Vol. VI, No. 2, pp. 33-48.
- romanosky, sasha, 2012, **empiricalanalise of data brach litigation**. No. 29,pp.1-25.
- Swire, Peter; Ahmad, Kenesa, 2012, **Encryption and Globalization**, Columbia Science and Technology Law Review, Vol. 23, No. 157, pp. 416 - 481.
- Wang, Minyan, 2006, **The Impact of Information Technology Development,** Journal of Law and Technology, Vol. 15, No. 3, pp. 1-37.