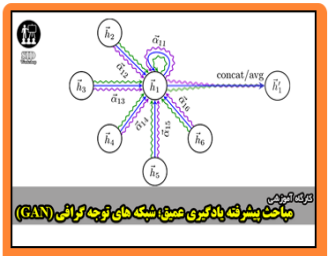
کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین مکالمه روزمره انگلیسی

کارگاه آنلاین آموزش استفاده از وب آو ساینس



مباحث پیشرفته یادگیری عمیق؛
شبکه های توجه گرافی
(Graph Attention Networks)

امنیت در فضـای سایبری با تأکید بر پیشگیری وضعی و اجتماعی از جرایم در فضای سایبری

زهرا بذرگر[1]، علی ناصرزاده[2]

چکیده

ساختار و فضای نامحدود اطلاعاتی اینترنت و نیز همگانی، بی‌کنترل و بدون محدودیت بودن این فضا ضمن آنکه دستاوردهای مهمی را برای بشر بوجود آورده سبب شده است که فضای سایبری به‌عنوان یکی از پر مخاطره ترین فضاهای دریافت اطلاعات در جوامع بشری معرفی شـود. ایـن گسترش سرسام آور مشکلات و آسیب‌های عدیده‌ای در زمینه‌های حقوقی، امنیتی، اخلاقی، فرهنگی و... برای کاربران و جوامع بوحود می‌آورد. که بعضا سبب وقوع یک سری از جرایم یا به تعبیری «جرایم سایبری» می‌شود. ازطرفی راه حل مناسبی نیز برای پیشگیری این مشکلات ارائه نمی‌شود. به اعتقاد نگارنده راه حل مناسب آن است که تدبیری اتخاذ شود که ابزار ارتکاب جرم را از مجرم سلب کند. به عبارت دقیق تر سیاست پیشگیری از جرایم بهترین سیاست جنایی جهت تامین امنیت فضای سایبر است. در این میان پیشگیری وضعی و اجتماعی یکـی از اقـدامات مهـم محسـوب می‌شود. فرضیه‌ای که در پی اثبات آن هستیم آن است که با توسل به پیشگیری‌های غیر کیفـری می‌توان عدم امنیت در فضای سایبر را مدیریت کرد. در همین راستا با سوالاتی از قبیل:۱-چگونگی فراهم کردن امنیت در فضای سایبر؟۲- در مسیر اجرای پیشگیری غیر کیفری با چه محدودیت هایی مواجه هستیم؟ با اثبات فرضیه و پاسخ به سوالات و... به این نتیجه رسـیدیم کـه بـا توجـه بـه محدودیت‌های حاکم بر پیشگیری‌های غیرکیفری محرز شد که جهت تامین امنیت راه دشواری در پیش است در عوض آثار مثبت و سازنده آن به مراتب بیشتر از ضمانت اجراهای کیفری می‌باشد. روش بررسی این تحقیق تحلیلی وتوصیفی می‌باشد.

کلیدواژه‌ها: فضای سایبری، امنیت فضای سایبری، پیشگیری غیر کیفری، پیشگیری وضعی

[1]. کارشناس ارشد، پژوهشگر / z.bazrgar@gmail.com

[2]. کارشناس، پژوهشگر

۱-مقدمه

بخشی از واقعیت‌های زندگی امروز ما در فضای مجازی تحقق می‌یابد که ویژگی‌های آن با دنیای فیزیکی متفاوت است.ورود رایانه به دنیای انسانها،شیوه زندگی آنها را دگرگون ساخته وبسیاری از معضلات جامعه بشری را با سرعت ودقتی بالا مرتفع ساخته است.

در این فضا،ما اوقات فراغت وزندگی خود را با مردمی با ارزش‌ها و وابستگی‌های متفاوت و گاه متعارض سپری می‌کنیم.بخش قابل توجهی از فعالیت‌های سیاسی،اقتصادی،فرهنگی و اجتماعی ما را در این فضای ارتباطی شکل می‌گیرندInda&Rosalo(،52،2002)

در فضای سایبر،مفایم فضا،جامعه و کنترل،ابعاد جدید و متفاوتی می‌یابند.در فضای سایبر،جامعه تبدیل به مفهومی بدون جغرافیا می‌شود.جامعه در فضای سایبر از افرادی شکل می‌گیرد که هیچکدام یکدیگر را نمی شناسند.روابط اجتماعی در این فضا از سطح متفاوتی از فضای واقعی برخوردار است.در نتیجهمی توان از شکل گیری جامعه ای مجازی و شبکه ای در کنار جامعه واقعی صحبت کرد که بستر وقوع رویدادهای متفاوت است.شهروندان این جامعه ی مجازی در فضای فرهنگی متکثر وبدون مرز و با هویت پیوندی،اجتماعی می‌شوند.(عاملی،۱۳۸۲،۲۸)

هرچند که یارانه برای جامعه بشری دستاوردهای بسیاری داشته است،اما فضای سایبر نیز همانند دیگر عرصه‌های زندگی اجتماعی نتوانسته است از آسیب وگزند سو ءاستفاده گران در امان باشد.برای مثال انتشار تصاویر مستهجن افراد وخصوصا کودکان در این محیط،در عین حالی که وسیله سودآوری برای ارائه کنندگان این تصاویر گشته،برای خواستاران ارضای غرایز جنسی دنیای آزاد فراهم آورده که هر لحظه خواستند می‌توانند تمایلات غریزی خود را فرو بنشانند.محیط سایبر همچنین دنیای آزاد برای کسانی است که قصد ایذاء واضرار افراد را دارند:کلاهبرداری رایانه ای،جعل،پورنوگرافی هویت،مزاحمت‌های رایانه ای،جرایم علیه حساب پست الکترونیک افراد،دسترسی غیر مجاز به ذاذه‌ها وسیستم‌های رایانه ای اشخاص،سرقت اطلاعات و... همگی از مصادیق جرایمی هستند که یارانه امکان ارتکاب آنها را بسیار افزایش داده است.چنانچه آسیب و جرایم سایبری در سطح جهانی به مسئله مهمی برای افراد،خانواده ها،سازمان‌ها وشرکت‌های بزرگ تجاری تبدیل شده و همه ملت‌ها را به فکر چاره ای برای مبارزه با این آسیب‌های خطرناک وزیانبار انداخته است به طوری که در جوامع مختلف به جرم انگاری وپیش بینی تدابیر کیفری(مجازات)در این زمینه پرداخته اند.اما با توجه به ناکارآمدی تدابیر کیفری و غیر قابل شناسایی بودن مجرمین سایبری،پیشگیری از وقوع این جرایم وآسیب ها،حفظ امنیت سایبری و به عبارتی به کار گیری پدافند غیرعامل جایگاه ویژه می‌یابد.در این نوشتار سعی بر آن است تا انواع جرایم سایبری را شناسایی کرده،شیوه‌های متفاوت پیشگیری(وضعی واجتماعی)را شرح داده ونقش آن را در کاهش وجلوگیری از وقوع

چنین جرایمی بررسی می‌کنیم.

۲-انواع جرایم سایبری

-فحشا وهرزه نگاری

-هک کردن

-پخش وانتشار ویروس

-کلاهبرداری اینترنتی

-سو ءاستفاده مالی از کارت‌های اعتباری

-قماربازی اینترنتی

-تروریسم اینترنتی

۳-پیشگیری

هم اکنون اهمیت تدابیر پیشگیرانه بر کسی پوشیده نیست زیرا علاوه بر اینکه از بروز ناهنجاری‌ها و آسیب‌های گوناگون جلوگیری می‌کند.انواع هزینه‌های مربوط به اعمال هرگونه ضمانت اجرای کیفری را در تمام مراحل رسیدگی تا مجازات به حداقل مر رساند.ودر جرایم سایبری به علت پوشیده ماندن اعمال ارتکابی وعدم کشف آن‌ها که ناشی از عدم نظارت دقیق و موثر بر محیط سایبر است و نیز این موضوع که آثار جرایم ارتکابی در این محیط،معمولا باقی نمی ماند،تدابیر پیشگیرانه مهمترینااقدام در کاهش وجلوگیری از بروز جرایم وآسیب‌های سایبری به شمار می‌رود.در ادامه به دو نوع پیشگیری که عبارت است از پیشگیری وضعی واجتماعی که مهمترین نوع پیشگیری می‌باشد می‌پردازیم.

۳-۱- پیشگیری اجتماعی

پیشگیری اجتماعی مجموعه تدابیرآموزشی،فرهنگی،اقتصادی واحتماعی هستند که برای سالم سازی محیط وحذف یا کاهش عوامل اجتماعی جرم مورد استفاده قرار می‌گیرند.(نجفی ابرند آبادی،۱۳۸۲،۱۲۴۶)

رویکرد پیشگیری اجتماعی معطوف به علل وعوامل بنیادین وقوع جـرم اسـت وشـرایط اجتمـاعی جـرم زا،مشارکت جامعه ونهادهای آن برای مقابله با پدیده مجرمانه وارتباط میان کارایی وتاثیر گذاری نهادهـای جامعوی بر وقوع جرایم در آینده مورد توجه قرار می‌گیرد.این نوع از پیشگیری شامل تمامی تـدابیری اسـت که بر انواع محیط‌های پیرامون فرد تاثیر می‌گذارند.تمامی این محیط‌ها در فرایند جامعه پـذیری فـرد نقـش دارند و دارای کارکردهای اجتماعی هستند.پیشگیری اجتماعی با ایجاد تغییرات واصلاحاط در فـرد وجامعـه به دنبال جلوگیری از جرم به صورت پایدار و همیشگی است ومـی کوشـد تـا اعضـای جامعـه را از طریـق آموزش،تربیت،تشویق وتنبیه با نظام اجتماعی و فرهنگی آشنا وهمنوا کند.(شاطری پور،۱۳۸۸،۸۹)

۳-۲- آموزش

آگاه سازی جامعه نسبت به آسیب‌ها وچالش‌های موجود در فضای اینترنت و آموزش شیوه‌های صحیح مقابله با این آسیب‌ها یکی از مهمترین راه‌های پیشگیری از وقوع جرایم در این حوزه می‌باشد. چنانچه بتوان توصیه‌ها وآموزش‌های لازم را به والدین منتقل وآنها را با خطرات پیش رو فضای سایبر آشنا کرد،می توان تا حدود زیادی از وقوع برخی جرایم جلوگیری کرد.برای مثال برنامه آموزشی والدینی که فرزندانشان با اینترنت کار می‌کنند،می تواند حاوی این نکات باشد:ایجاد حس مسئولیت پذیری و توانایی انتخاب گزینه‌های سالم به هنگام استفاده از اینترنت،تصمیم گیری به جا و مناسب درباره محتوایی که قرار است مشاهده کنند وآموزش نحوه رویارویی با محتوای نا مناسب که ممکن است مشاهده کنند وکاهش عواقب آن.در حقیقت ابتدا به والدین چگونگی اتخاذ این رهیافت‌ها را نسبت به کودکانشان آموزش داد.(Thornburgh&Lin،218،2004)

در آموزش‌های عمومی تاکید بر رعایت اخلاق بسیار مهم وتعیین کننده است.

بررسی سیاست‌های اعمال شده از جانب کشورهای پیشرو،بیانگر این مهم است که در این کشورها،آگاه سازی عموم نسبت به امنیت واخلاق در فضای رایانه اریا،طی یک برنامه ملی ویک پارچه وبا مشارکت نهادهای سیاستگذار اجرایی،قضایی،بنگاههای تجاری ورسانه‌های عمومی صورت می‌پذیرد.(محسنی، ۱۳۷۰،۲۵)

۳-۳- ارتقای سطح فرهنگ واخلاق

موازین وضوابط اخلاقی در چارچوب رایانه وبه ویژه جرایم رایانه ای از خصوصیات خاصی برخوردار است:"افرادی که به ندرت مقررات و قوانین اخلاقی و قانون را زیر پا می‌گذارند،بدون تردید دست به دزدی نرم افزار نمی زنند.انقلاب رایانه چنان سریع روی داد که ارزش‌های فرهنگی واخلاقی،فرصتی برای تطبیق با آن نیافته اند."(ابراهیم زاده پاشا،۱۳۷۵،۵۳۳)

برخلاف علوم رایانه،علوم ورشته‌های دیگر فرصت بیشتری برای اصول وضوابط اخلاقی در ارتباط با تحولات جدید خود داشته اند.برای مثال ضوابط اخلاقی در پزشکی،حسابداری،حقوق ومهندسی به خوبی جا یافته است.مسایل اخلاقی ویژه رایانه،از ویژگی‌های منحصر به فرد رایانه‌ها ونقشی که بر عهده دارند سرچشمه می‌گیرد.عدم رضایت ضوابط اخلاقی گاهی به شکل تجاوز به حقوق خصوصی وفردی بروز می‌کند ویا ممکن است تجاوز به حق تالیف باشد.ویا تحت عناوین مجرمانه دیگری قرار گیرد که در برخی از کشورها موضوع قوانین خاصی در این مورد است.(پاکزاد، ۱۳۸۰، ۵۵.۵۶)

بنابراین در حال حاضر مهمترین نکته در این مورد،اشاعه فرهنگ صحیح به کارگیری تکنولوژی رایانه وتوسعه معیارهای اخلاقی است.تا زمانی که این کار صورت نگیرد،نمی توان انتظار داشت تا مردم خود را پایبند به آن بدانند.

۴-پیشگیری وضعی

مجموعه تدابیر کنشی است که وضعیت پیش بزه کاری را به ضرر مجرم تغییر داده وبزه دیدگان احتمالی وافراد وسیبل‌های در معرض آسیب را حمایت میکند.(نجفی ابرند آبادی،۱۳۸۲،۱۲۴۶)

۴-۱- تدابیر اداری و سازمانی

امنیت سازمانی و اداری شامل تعیین یک خط مشی کلی امنیتی وفراهم ساختن روش‌های اجرای آن می‌شود.گرچه تدابیر ویژه امنیت اداری بر حسب حجم و ماهیت کارهای انجام شده به وسیله سازمان‌ها بسیار متغییرند،اما حداقل نیازهای آن عبارت اند از:

الف-ارتقاء وبسط روش هایی که شناسایی خطرهای ممکن را تضمین کند.

ب-تعریف وظایف امنیتی افراد وتخصیص مسئولیت‌های لازم ومقتضی.

ج-تعیین مناطق ممنوعه

د-به کارگیری روش‌های اعطای مجوز

ه-مشخص کردن وابستگی‌های خارجی و قراردادی

و-تهیه برنامه‌های احتیاطی(دبیر خانه شورای انفورماتیک،۷۴)

یکی از معضلات بزرگ برای ادارات و سازمان‌های ذیربط،تعدیات وتجاوزات کارکنان اخراجی از سوی این ادارات است.مثلا یکی از کارمندان اخراجی یک شرکت آمریکایی،چند روز پس از اخراج از شرکت،به درون سیستم شرکت محل کار سابق خود رخنه کرد وتوانست با کارگزاردن یک بمب ساعتی(ویروس بمب)که در سیستم فروش شرکت کار می‌کند۱۶۸۰۰۰رکورد یا اطلاعات مربوط به کمیسیون‌های فروش را ماهی یک بار پاک کند.او در واقع یک برنامه نویس رایانه ای بود که به سادگی قادر بود رمزهای عبور سیستم را که خود قبلا بوجود آورده بود،بشکند.برای جلوگیری از چنین وضعیتی تنها به کارگیری چند قاعده اساسی در مواردی که کارمندی اخراج شود کافی است:(همان،۷۵)

الف-به کارمندانی که از کار برکنار شده اند،اجازه دسترسی به هیچ یک از اطلاعات ویا هیچ بخشی از سیستم اطلاعاتی ماشینی را ندهید.

ب-هرگونه رمز عبور را که چنین کارمندی از آن اطلاع داشته،عوض نمایید و رمز جدید را در اختیار کارکنان مجاز مربوطه قرار دهید.به این ترتیب کارمند ارکنار شده،دیگر قادر نخواهد بودبا رمزهایی که می‌داند وارد سیستم شود.

ج-سعی کنید که از هرگونه امکان دستیابی این قبیل افراد به رمزهای مربوطه به به افراد دیگر سازمان نیز مطلع شوید ودر صورتی که معلوم شد آن‌ها این رمزها را می‌دانسته اند تمامی آنها را عوض کنید.(عرب مازاد،۴۷)

۴-۲- تدابیر فنی

روش‌های فنی عبارت از آن دسته اقداماتی هستند که در قلمرو یارانه برای امنیت سیستم رایانه ای به کار گرفته می‌شوند.البته ایجاد روش فنی،ارتکاب جرایم رایانه ای را به طور کلی محو نمی کند و البته روشن است که چنین انتظاری هم از این روش غیر معقول خواهد بود.از یک طرف نمی توان اقدامات فنی را به تمام زمینه‌ها گسترش داد واز سوی دیگر در مقابل به کارگیری این روش،مرتکبین جرایم رایانه ای قرار دارند که می‌خواهند این اقدامات را خنثی سازند وبعضا هم موفق به این کار می‌شوند.(Neitzke،95)

همچنین یا داور می‌شویم که گاه از به کار گیری تدابیر فنی به وسیله صاحبان سیستم‌های رایانه ای خود داری می‌شود.این گروه برای خود دلایلی دارند،مثلا تعبیه بعضی از ابزارهای فنی،سبب افزایش هزینه‌ها می‌شود.(شریفی،۱۳۷۹،۲۰۳)

۴-۳- رمزگذاری رایانه

یکی از مولفه‌های اساسی برای تشخیص شخص متجاوز،اثبات هویت فرد است استفاده از پسورد،امنیت متداول برای سیستم شبکه شامل سرورها،مسیر پیام‌ها تا رسیدن به هدف و دیواره‌های آتش را افزایش می‌دهد.اساسا در همه سیستم‌ها برای دستیابی به سیستم رایانه،در خواست نام کاربری و پسورد برنامه ریزی شده است. این امر شناسایی کاربر را میسر می‌سازد پسورد باید با فاصله منظم تغییر یابد و باید عدد باشد و به سختی شناسایی شود.(سلیمانی،یوسفعلی،۱۳۸۹،۱۰۸)

۴-۴- یافتن روزنه شبکه

مدیران شبکه باید روزنه‌های قابل نفوذ شبکه خود را قبل از سارقان شناسایی کنند.برخی از شرکت‌ها ی طراح شبکه رایانه ای از روزنه‌های امنیت در تولیداتشان آشنا نیستند.این سازمان‌ها باید برای کشف روزنه‌های امنیت ونقاط ضعف شبکه خود به سختی کار کنند ویافته هایشان را زمانی که اثبات شدند،گزارش کنند(همان،۱۰۹)

۴-۵- استفاده از برنامه‌های مرورگر شبکه

ابزاری برای مدیریت امنیت با نام یونیکس به صورت رایگان در اینترنت وجود دارد.این برنامه‌های مفید،صرف نظر از خدمات وسیستم عملیاتی که برای میزبان فراهم می‌کند.اطلاعات آنها را در یک شبکه جمع آوری و مرور کرده وآسیب‌های شناخته شده از قبیل وجود ویروسها وضعف امنیت را شناسایی می‌کنند.محصول سودمند دیگری نیز بنام کپس وجود دارد که پسوردهای ضعیف و فایل‌های مضر وتاریخ فایل‌های کلیدی را اسکن می‌کند.(همان،۱۳۸۹،۱۰۹)

۴-۶- استفاده از برنامه‌های اعلام خطر نفوذ

نظربهاینکهتشخیصوبستنراههایاینفوذبهسیستم،اهمیتبالاییدار،قراردادنبرخینرمافزارهایمراقب،امریضروریاست.بر خیبرنامههایاعلامخطرنفوذوجوددارند،کهفعالیتهایمشکوکراشناساییوبهمنظورهرگونهاقداماتلازمگزارشمیکند.ا ینگونهنرمافزارهابایدبهطوردائمیاجراشوندتاهمهیحرکتهایغیرمعمولدرشبکهفوراکنترلومتوقفشود.(همان،۱۰۹، ۱۳۸۹)

۵- نتیجه گیری

هرچند که یارانه برای جامعه بشری دستاوردهای بسیاری داشته است،اما فضای سایبر نیز همانند دیگر عرصه‌های زندگی اجتماعی نتوانسته است از آسیب وگزند سو ءاستفاده گران در امان باشد و تبدیل به معضلی شده است که در نظام‌های حقوقی مختلف مورد جرم انگاری قرار گرفته است و واکنش‌های کیفری(مجازات)برای آن پیش بینی گردیده است.اما گسترش روز افزون فساد حاکی از ناکارآمدی اقدامات کیفری است. دراین میان اقدامات غیر کیفری چون پدافند غیرعامل می‌توان راه گشا باشد،از جمله این اقدامات تدابیر پیشگیری وضعی و اجتماعی از این گونه جرایم می‌باشد

بعضی وقت‌ها می‌توانیم بدون اینکه الزاما کار خاصی را درمورد بزهکاران انجام دهیم،از وقوع جرایم خاص پیشگیری نماییم یا حداقل آن را کاهش دهییم.بعضی وقت‌ها ما می‌توانیم از طریق تغییر برخی جنبه‌های مربوط به ساختار فرصت جرایم،از وقوع آن‌ها پیشگیری نماییم.مسدود کردن راه دسترسی مجرم به هدف،عملی کردن افکار و اندیشه‌های مجرمانه را برای وی بسیار سخت و مشکل می‌سازد وهمین امر جذابیت فرصت مجرمانه را برای بزهکار کمتر می‌کند.

از جمله تدابیر پیشگیرانه اجتماعی از وقوع جرایم سایبر،آموزش و ارتقای سطح فرهنگ و اخلاق می‌باشد آگاه سازی جامعه نسبت به آسیب‌ها وچالش‌های موجود در فضای اینترنت و آموزش شیوه‌های صحیح مقابله با این آسیب‌ها یکی از مهمترین راه‌های پیشگیری از وقوع جرایم در این حوزه می‌باشد.

از جمله اقدامات پیشگیرانه وضعی از جرایم سایبر عبارتند از: تدابیر اداری و سازمانی، تدابیر فنی، رمزگذاری رایانه، یافتن روزنه شبکه، استفاده از برنامه‌های مرورگر شبکه، استفاده از برنامه‌های اعلام خطر نفوذ

۶- منابع

۱- ابراهیم زاده، پاشا، (۱۳۸۱) حقوق مولفین یارانه ای، پایان نامه دوره کارشناسی ارشد، دانشگاه شهید بهشتی، دانشکده حقوق

۲- پاکزاد، بتول، (۱۳۸۰)، جرایم رایانه ای، پایان نامه دوره کارشناسی ارشد، دانشگاه شهید بهشتی

۳- دبیرخانه شورای عالی انفورماتیک، نشریه بین المللی سیاست جنایی

۴- سلیمانی، مجید، یوسفعلی، حجت، (۱۳۷۹)، جرم سایبری، ردیابی، پیشگیری

۵- شاطری پور، شهیده، (۱۳۸۸)، پیشگیری از وقوع جرم در کنوانسیون پالرمر ۲۰۰۰ و کنوانسیون مریدا ۲۰۰۳، فصلنامه مطالعات پیشگیری از وقوع جرم، نشر تحقیقات کاربردی پلیس پیشگیری نیروی انتظامی

۶- شریفی، مرسده، (۱۳۷۹)، جرایم رایانه ای در حقوق جزای بین الملل، پایان نامه دوره کارشناسی ارشد، دانشگاه آزاد اسلامی

۷- عاملی، سعید رضا، (۱۳۸۲)، دو جهانی شدن و آینده جهان، کتاب ماه علوم اجتماعی،

۸- عرب مازار، محمد، کابوس و ویروس‌های کامپیوتری

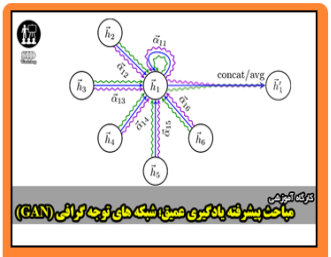
۹- محسنی، منوچهر، (۱۳۷۰)، شبکه‌های اطلاعاتی اینترنت و ویژگی‌ها و تاثیرات اجتماعی فرهنگی

۱۰- نجفی ابرند آبادی، علی حسین، (۱۳۸۲)، تقریرات درس جرم شناسی، حمید بهره مند و محمد مصور، دانشگاه امام صادق(ع)

کارگاه های آموزشی مرکز اطلاعات علمی جهاد دانشگاهی

کارگاه آنلاین مکالمه روزمره انگلیسی

کارگاه آنلاین آموزش استفاده از وب آو ساینس



مباحث پیشرفته یادگیری عمیق؛ شبکه های توجه گرافی (Graph Attention Networks)