گزارش کامپیوتر

ISSN 1735 - 4404

ماهنامه انجمن انفورماتیک ایران

سال چهل و دوم، فروردین و اردیبهشت ۱۳۹۹، شمارهٔ ۲۴۷

ماهنامهٔ انجمن انفورماتیک ایران
(فعلاً هردوماه یکبار منتشرمی شود.)

گزارش کامپیوتر

سال چهل و دوم، فروردین و اردیبهشت ۱۳۹۹، شمارهٔ ۲۴۷

صاحب امتیاز: انجمن انفورماتیک ایران

مدیر مسئول و سردبیر: ابراهیم نقیب‌زاده مشایخ

مقاله‌ها و گزارشهای تالیفی یا ترجمه خود را برای گزارش کامپیوتر بفرستید. مطالب ارسالی را با خط خوانا (یا ماشین شده) بر یک روی کاغذ بنویسید فاصله کافی برای افزودن اصلاحات ویرایشی در بین خطها و حاشیه در نظر بگیرید. در صورت ارسال مطلب ترجمه شده، یک نسخه از اصل مطلب را نیز ارسال دارید. شکلها باید با روان‌نویس مشکی ترسیم و به‌صورت آماده چاپ ارسال شوند. مطالب ارسالی پس فرستاده نمی‌شوند.

مسؤولیت مطالب گزارش کامپیوتر با نویسندگان است و لزوماً نشان‌دهنده نظر انجمن انفورماتیک ایران نیست. ذکر نام شرکتها و محصولات در مطالب گزارش کامپیوتر برای ارائه اطلاع به خوانندگان است و نباید به معنی تائید انجمن از آنها تلقی شود.

سازمان آگهی‌ها: مهناز خاوندکار
تلفکس : ۸۸۳۲۸۴۱۷-۲۱
حروفچینی : انجمن انفورماتیک ایران
لیتوگرافی: نگارین پرتو ۷۷۵۳۰۳۰۷
چاپ علوی تهران : ۶۶۷۰۱۵۲۷
خ جمهوری ، ۳۰ تیر ، کوچه مصری پور ، پلاک ۲۵۶

فراخوان مقاله دومین ۳ و ٤ دی‌ماه ۱۳۹۹

کنفرانس ملی انفورماتیک ایران

پژوهشکده علوم کامپیوتر، پژوهشگاه دانش‌های بنیادی، فرمانیه، تهران

انجمن انفورماتیک ایران

پژوهشگاه دانش‌های بنیادی

پژوهشگاه دانش‌های بنیادی دومین کنفرانس ملی انفورماتیک ایران را با همکاری انجمن انفورماتیک ایران و با هدف رشد و توسعه دانش انفورماتیک برگزار می‌کند. تأکید این کنفرانس بر جنبه‌های بنیادی، کاربردی، راهبردی و توسعه‌ای انفورماتیک است که از سودمندی خاص در سطح کشور برخوردارند. از تمامی پژوهشگران، دانشگاهیان و صنعتگران دعوت می‌شود تا با ارسال مقاله و شرکت در کنفرانس با تبادل یافته‌های پژوهشی و کاربردی خود موجب پرباری و اثربخشی کنفرانس در راستای اهدافش باشند.

زمینه‌های علمی کنفرانس

امسال کنفرانس ملی انفورماتیک ایران در چهار شاخه اصلی زیر مقالات را بررسی و برای ارائه (شفاهی و پوستری) و چاپ در مجموعه مقالات انتخاب خواهد کرد.

سیستم

- معماری کامپیوتر
- سیستم حافظه و ذخیره سازی داده
- شبکه کامپیوتری
- امنیت داده و کامپیوتر
- پایگاه داده
- سیستمهای تعبیه شده و کم توان
- سیستمهای بی درنگ
- پردازش با کارایی بالا
- ارزیابی و تحلیل کارایی
- سیستمهای عامل
- زبانهای برنامه سازی
- مهندسی نرم افزار
- پردازش موبایل
- رایانش ابری
- دیگر موضوعهای مرتبط با این شاخه

هوش مصنوعی

- هوش مصنوعی
- یادگیری ماشین
- رایانش نرم
- شناسایی الگو
- داده کاوی
- پردازش زبان طبیعی
- بینایی ماشین و پردازش تصویر
- وب و بازیابی اطلاعات
- دیگر موضوعهای مرتبط با این شاخه

تئوری

- طراحی و تحلیل الگوریتم‌ها
- هندسه محاسباتی
- الگوریتم‌های تقریبی و تصادفی
- پیچیدگی محاسبات
- الگوریتمها کوانتومی
- الگوریتم‌های موازی و توزیع‌شده
- منطق و اعتبارسنجی
- روش‌های صوری
- دیگر موضوعهای مرتبط با این شاخه

زمینه‌های بین رشته‌ای

- پردازش داده‌های کلان
- بیوانفورماتیک
- گرافیک کامپیوتری
- اقتصاد و محاسبات
- تعامل انسان و کامپیوتر
- رباتیک
- مصورسازی
- اینترنت اشیا
- زنجیره‌های بلوکی
- دیگر موضوعهای بین رشته‌ای

رؤسای کنفرانس:

م.ج. ا. لاریجانی، رئیس پژوهشگاه دانش‌های بنیادی

ا. ناظمی، رئیس انجمن انفورماتیک ایران

دبیر کنفرانس:

پ. لطفی کامران، پژوهشگاه دانش‌های بنیادی

کمیته علمی کنفرانس:

ح. سربازی‌آزاد، دانشگاه صنعتی شریف و پژوهشگاه دانش‌های بنیادی (دبیر کمیته)

مسئولین شاخه‌های علمی:

م. مدرسی، دانشگاه تهران (شاخه سیستم)

م. ابراهیمی مقدم، دانشگاه شهید بهشتی (شاخه هوش مصنوعی)

ع. زارعی، دانشگاه صنعتی شریف (شاخه تئوری)

م. عبدالهی‌ازگمی، دانشگاه علم و صنعت (شاخه زمینه‌های بین‌رشته‌ای)

کمیته اجرایی کنفرانس:

س. گرگین، سازمان پژوهش‌های علمی و صنعتی ایران (کارگاه‌ها)

ش. علیپور، پژوهشگاه دانش‌های بنیادی (تبلیغات)

ن. رهبانی، پژوهشگاه دانش‌های بنیادی (اینترنت)

ا. ا. لاریجانی، پژوهشگاه دانش‌های بنیادی (میزگردها)

م. رضایی، پژوهشگاه دانش‌های بنیادی (ارتباط با صنعت و امور حامیان)

م. اسدی، پژوهشگاه دانش‌های بنیادی (انتشارات)

ف. بهاری‌فرد و س. حسین‌قربان، پژوهشگاه دانش‌های بنیادی (پژوهش دانشجویان دکترا)

ح.ر. شهرابی‌فراهانی، پژوهشگاه دانش‌های بنیادی (امور اجرایی)

تاریخ‌های مهم:

مهلت ارسال مقالات به کنفرانس ..... ۱۵ مهر ۱۳۹۹

اعلام قبولی یا رد مقالات ..... ۱ آذر ۱۳۹۹

مهلت ثبت نام و ارسال نسخه نهائی مقالات ..... ۲۰ آذر ۱۳۹۹

مهلت ارسال مقالات پژوهش دانشجویان دکترا ..... ۱۵ آبان ۱۳۹۹

اعلام قبولی یا رد مقالات پژوهش دانشجویان دکترا ..... ۱ آذر ۱۳۹۹

نشانی دبیرخانه کنفرانس:

تهران، خیابان دکتر لواسانی، تقاطع کامرانیه-فرمانیه، نبش خیابان فربین، پژوهشگاه دانشهای بنیادی، پژوهشکده علوم کامپیوتر.

تماس با کنفرانس:

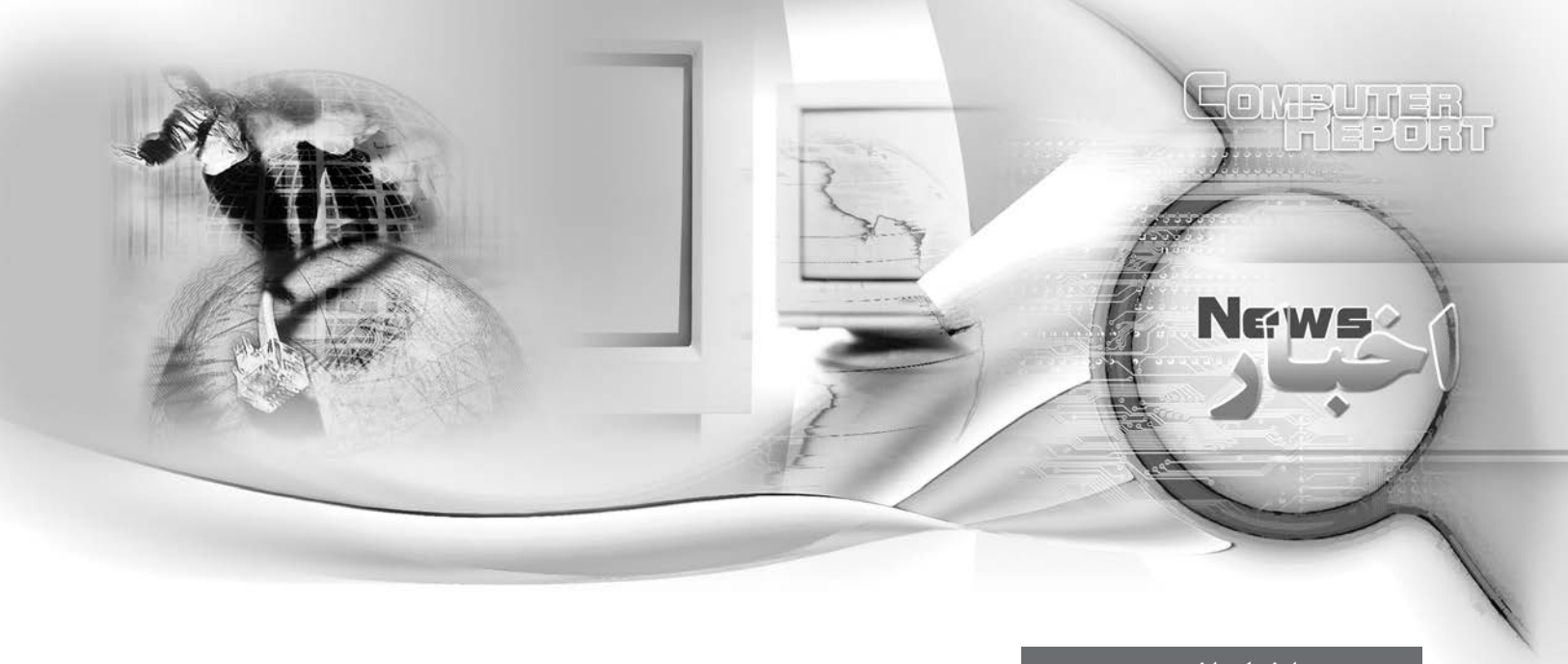
آدرس پست الکترونیکی..... nic@ipm.ir

تلفن..... ۲۲۸۲۵۳۵۴

نمابر..... ۲۲۸۲۵۴۵۴

مقالات باید فقط به زبان فارسی تهیه و ارسال شوند و نشان دهنده کار جدید بوده و قبلاً در مجموعه مقالات کنفرانسهای دیگر و یا در مجلات منتشر نشده باشند. ارسال همزمان مقاله به دیگر کنفرانس‌ها و مجلات مجاز نیست و موجب رد شدن مقاله (در هر مرحله که مشخص شود) خواهد شد. لازم است ارسال مقالات در قالب PDF (حداکثر ۶ صفحه) و چکیده آن در قالب Word (یک صفحه) مطابق قالب صفحه‌بندی که در سایت کنفرانس در دسترس است، فقط به صورت الکترونیکی و از طریق سایت کنفرانس انجام شود. برای هر مقاله پذیرفته شده، حداقل یکی از مؤلفین باید ثبت‌نام عادی کرده و مقاله را در کنفرانس ارائه کند. ضمنا پس از برگزاری کنفرانس، مقالات منتخب کنفرانس برای چاپ در یک شماره ویژه مجله علوم رایانشی در نظر گرفته خواهند شد.

http://cs.ipm.ac.ir/nic/1399



اخبار انجمن

چاپ کتاب مهارت‌های نرم

کتاب «مهارت‌های نرم: راهنمای زندگی تولیدکنندگان نرم‌افزار» در اسفند ماه گذشته از سوی انجمن انفورماتیک ایران منتشر شد. این کتاب توسط آقای ابراهیم نقیب‌زادهٔ مشایخ ترجمه شده و کلیهٔ حقوق آن به انجمن انفورماتیک ایران واگذار شده است. کتاب مهارت‌های نرم با حمایت مالی شرکت پویا انتشار یافته است که بدین وسیله از مدیریت محترم آن شرکت صمیمانه سپاسگزاری می‌گردد.

برگزاری وبینار علم داده‌ها

انجمن انفورماتیک ایران و انجمن آمار ایران مشترکاً وبیناری را با عنوان «علم داده‌ها» در تاریخ چهارشنبه ۲۱ خرداد ۹۹ از ساعت ۱۸ تا ۲۰ برگزار کردند.

در این وبینار، دو سخنرانی به شرح زیر برگزار گردید:

۱- عنوان سخنرانی: علم داده‌ها

سخنران: آقای دکتر افشین آشفته، مدرس علم داده در دانشکده مدیریت اطلاعات و علوم داده دانشگاه نُوا در کشور پرتغال

۲- عنوان سخنرانی: مقدمه‌ای دوستانه در یادگیری عمیق

سخنران: آقای دکتر هادی فراهانی، استادیار و سرپرست گروه علوم داده‌ها و کامپیوتر دانشگاه شهید بهشتی

لازم به ذکر است که استقبال خوبی از برگزاری این وبینار به عمل آمد و بیش از ۲۰۰ نفر از نقاط مختلف کشور در آن حضور یافتند.

پایان همکاری خانم بهاری با انجمن

خانم مهسا بهاری که ظرف ۹ سال گذشته با دفتر انجمن همکاری داشت و در چند سال اخیر مسئول روابط عمومی انجمن بود، از اوّل تیرماه سال جاری در سازمان دیگری ادامهٔ فعالیت خواهد داد.

انجمن انفورماتیک ایران بدین وسیله از خانم بهاری به خاطر صداقت، سختکوشی و همکاری صمیمانه‌ای که با انجمن داشت قدردانی کرده و برای او موفّقیت آرزو می‌کند.

لازم به ذکر است که خانم یاسمن فرجی از این پس مسئولیت روابط عمومی انجمن را برعهده خواهد داشت.

همکاری با انجمن آموزش مهندسی ایران

انجمن آموزش مهندسی ایران، شمارهٔ ۲۴۶ ماهنامهٔ گزارش کامپیوتر را که به‌صورت الکترونیکی منتشر شده بود از طریق وبگاه خود (isee.ir) در اختیار اعضای آن انجمن و دیگر علاقه‌مندان قرار داد.

انجمن انفورماتیک ایران بدین وسیله از هیئت مدیرهٔ محترم آن انجمن قدردانی می‌نماید.

عضویت دائمی در انجمن

هیئت مدیرهٔ انجمن به‌منظور تأمین بودجهٔ لازم برای خریداری محلّی ثابت برای دفتر انجمن، نوع عضویت جدیدی را با عنوان عضو دائمی انجمن در نظر گرفته است.

بنابراین مصوّبهٔ هیئت مدیره که باید به تصویب مجمع عمومی آیندهٔ انجمن نیز برسد، اعضای حقیقی با پرداخت ۱۰ میلیون ریال و اعضای حقوقی با پرداخت ۵۰ میلیون ریال به عضویت دائمی انجمن درخواهند آمد.

تأمین محلّی ثابت برای دفتر انجمن، از هدف‌های دیرپای انجمن بوده است و هیئت مدیرهٔ فعلی انجمن تمام تلاش خود را برای تأمین بودجهٔ کافی برای خریداری محلّی بدین منظور به‌کار گرفته است.

امید است با حمایت اعضای انجمن از این طرح، بودجهٔ لازم برای برآورده ساختن این هدف مهم فراهم گردد.

تاکنون این افراد و شرکت‌ها به عضویت دائمی انجمن درآمده‌اند:

۱. آقای علی موفّقی اردستانی (عضو پیوسته)
۲. آقای وحید مجیدی (عضو پیوسته)
۳. آقای امیر خاوران (عضو پیوسته)
۴. شرکت توسعه و تجهیز فدک رایان (عضو حقوقی)

۵. شرکت تجارت سرور ماندگار (عضو حقوقی)
۶. شرکت گلرنگ سیستم (عضو حقوقی)
۷. شرکت ندا رایانه (عضو حقوقی)
۸. پژوهشگاه ارتباطات و فناوری اطلاعات (عضو حقوقی)
۹. شرکت خدمات انفورماتیک (عضو حقوقی)

چاپ شانزدهمین شمارهٔ مجلّهٔ علوم رایانشی

شانزدهمین شمارهٔ مجلّهٔ علوم رایانشی، نشریهٔ علمی انجمن انفورماتیک ایران، در خرداد ۱۳۹۹ منتشر شد.
در این شماره، ۶ مقاله به چاپ رسیده که چکیدهٔ آن‌ها در همین شمارهٔ گزارش کامپیوتر درج شده است.
متن کامل تمامی مقالات این شماره، همچون شماره‌های پیشین، از طریق وبگاه این مجلّه به نشانی csj.isi.org.ir در دسترس علاقه‌مندان قرار دارد.

چاپ پنجم کتاب کار عمیق

با استقبال گستردهٔ جامعهٔ فناوری اطلاعات کشور، کتاب کار عمیق، از انتشارات انجمن، در اسفند ماه ۱۳۹۸ به چاپ پنجم رسید.
شایان ذکر است که چاپ اوّل این کتاب در بهمن ماه ۱۳۹۶، چاپ دوم آن در اسفند ماه ۱۳۹۶، چاپ سوم آن در شهریور ماه ۱۳۹۷ و چاپ چهارم آن در اردیبهشت ۱۳۹۸ منتشر و در اختیار علاقه‌مندان قرار داده شده بود. هر چهار چاپ قبلی و چاپ پنجم با حمایت مالی شرکت پویا منتشر شده است.
فروش کتاب کار عمیق تنها از طریق دفتر انجمن انفورماتیک ایران (شماره تلفن ۶۶۴۱۲۸۶۱) و فروشگاه اینترنتی چاره (www.chare.ir) صورت می‌گیرد.

برگزاری دوره‌های تخصصی برای سازمان‌ها

انجمن انفورماتیک ایران آمادگی برگزاری دوره‌های زیر را برای کارشناسان سازمان‌های مختلف در محل آن سازمان‌ها دارد.
۱-کارگاه نیم روزه تدوین توافقنامه‌های سطح خدمات
۲-کارگاه یک روزه طراحی و استقرار پیشخوان خدمات
۳-کارگاه نیم روزه طراحی کاتالوگ خدمات
۴-کارگاه یک روزه ابزارهای مدیریت خدمات فناوری اطلاعات
۵-کارگاه نیم روزه برون‌سپاری خدمات و محصولات فناوری اطلاعات
۶-کارگاه نیم روزه همسوسازی IT با کسب وکار (IT Alignment) از طریق COBIT5
۷-کارگاه یک روزه راهبری فناوری اطلاعات (IT Governance) از طریق COBIT5
۸-کارگاه یک روزه راهبری فناوری اطلاعات(IT Governance)
۹-کارگاه نیم روزه مدیریت تدوام کسب و کار ISO2012:22301
۱۰-کارگاه نیم روزه راهبری فناوری اطلاعات و ITBSC
۱۱-کارگاه نیم روزه تدوین راهبرد خدمات فناوری اطلاعات
۱۲-کارگاه یک روزه مدیریت خدمات فناوری اطلاعات
۱۳-کارگاه سه روزه ITIL V3 Foundation 2011
۱۴-کارگاه یک روزه مدیریت مخاطرات فناوری اطلاعات
۱۵-کارگاه سه روزه دوره جامع COBIT5
۱۶-کارگاه نیم روزه توسعه نیازمندی‌ها مبتنی بر چارچوب CCMI-ACQ و استاندارد ISO/IEC29148:2011
۱۷- دورهٔ دو روزهٔ اسکرام مستر حرفه‌ای
ویژگی‌های این کارگاه‌ها عبارتند از :
• مشارکت گروهی، بحث و انجام سناریو، حل نمونه آزمون‌های امتحانی
• استفاده از مثال‌های مرتبط با حوزه فعالیت هر کسب وکار
• برگزاری دوره حداقل توسط دو مدرس دارای مدرک بین‌المللی
• برگزاری دوره در محل سازمان متقاضی
• ارائه مدرک شرکت در دوره از سوی انجمن انفورماتیک ایران
• ارائه مستندات آموزشی

علاقه‌مندان می‌توانند با دفتر انجمن انفورماتیک ایران (۶۶۴۱۲۸۶۱ و ۶۶۴۱۲۹۷۶) و یا نشانی پست‌الکترونیکی member@isi.org.ir تماس بگیرند.

اخبار ایران

دهمین سمپوزیوم بین‌المللی مخابرات

دهمین سمپوزیوم بین‌المللی مخابرات (IST 2020) با هدف اعتلای دانش و مهارت علمی و تخصصی در حوزهٔ ارتباطات و فناوری اطلاعات در تاریخ ۲۵ تا ۲۷ شهریور ۱۳۹۹ در پژوهشگاه ارتباطات و فناوری اطلاعات برگزار خواهد شد.
محورهای اصلی این سمپوزیوم عبارتند از:
• شبکه‌های آینده، سیستم‌ها و فناوری‌ها
• خدمات آینده
• سیاست‌ها و مقررات آینده

علاقه‌مندان برای دریافت اطلاعات بیشتر می‌توانند به وبگاه سمپوزیوم به نشانی ist2020.itrc.ac.ir مراجعه کنند.

فراخوان سی و چهارمین جشنوارهٔ بین‌المللی خوارزمی

سازمان پژوهش‌های علمی و صنعتی ایران، سی و چهارمین جشنوارهٔ بین‌المللی خوارزمی را با هدف ترویج فرهنگ کارآفرینی دانش‌بنیان و تجاری‌سازی نتایج تحقیقات، درج نهادن به مقام پژوهشگران و نوآوران و فناوران کشور و فراهم کردن بستر مناسب برای همکاری‌های علمی در سطح جهان برگزار می‌کند.
این جشنواره در ۱۷ گروه تخصصی، از جمله برق و کامپیوتر برگزار می‌شود. آخرین مهلت ثبت‌نام در این جشنواره، پایان شهریور ماه ۱۳۹۹ است.

علاقه‌منـدان بـرای کسـب اطلاعات بیشـتر می‌توانند به وبگاه www.irost.ir مراجعه کنند.

پنجمین دورهٔ مسابقات چالش‌های حوزهٔ فناوری اطلاعات و ارتباطات

دانشـگاه صنعتـی شـریف، پنجمیـن دورهٔ مسـابقات چالش‌های حوزهٔ فناوری اطلاعات و ارتباطات را با هدف شناسـایی افراد توانمند جویای کار در تابستان امسال برگزار می‌کند.
پنجمیـن دورهٔ ایـن مسـابقات بـا عنـوان «چالش‌هـای برنامه‌نویسـی» بـا تمرکـز بر زبان‌های جاوا، پایتـون، Node.js، .NET، PHP و Golang برگزار خواهد شد.
محل برگزاری این رویداد، صندوق نوآوری و شکوفایی ریاست جمهوری می‌باشد.
علاقه‌منـدان برای کسـب اطلاعات بیشـتر می‌توانند به وبگاه ictchallenge.sharif.ir مراجعه کنند.

اخبار جهان

عرضـهٔ تلفـن گالکسـی A71 سامسونگ

شـرکت سامسونگ تلفن نسل ۵ خود را به‌نام گالکسی A71 در آمریکا عرضه کرد. این تلفن ۶۰۰ دلار قیمت دارد که قیمت نسبتاً پائینی اسـت. دارای صفحهٔ نمایش ۶/۷ اینچی، ۱۲۸ گیگابایت حافظهٔ داخلی، ۶ گیگا بایت حافظهٔ اصلی و دستگاه شارژ کنندهٔ فوق سریع است. همچنین قابلیّت افزودن حافظهٔ اضافی تا یک ترابایت را دارد. این تلفن دارای آرایه‌ای از چهار دوربین است با عدسی اصلی ۶۴ مگاپیکسلی، عدسی زاویهٔ دید عریض ۱۲ مگاپیکسلی و دو عدسی عمقی و میکرو ۵ مگاپیکسلی.

سی‌نِت، ۱۵ جون ۲۰۲۰

فنّاوری‌هـای صوتـی در خدمـت شـکل‌دهی محـل کار در دوران پساکرونا

در حالی که محل‌های کار دسـت به گریبان بازگشـایی، همزمان با ادامهٔ بیماری دنیاگیر کوویـد ۱۹ هسـتند، فنّاوری‌هـای صوتی و رابط‌های بدون تماس می‌توانند پاسـخی به برقرارسازی محیط‌های کاری امن باشند.
معیارهـای فاصله‌گـذاری اجتماعی هنوز در اغلب کشـورها باید رعایت شـود و می‌تواند تا انتهای سـال نیز برای جلوگیری از شـیوع مجدّد ویروس کرونـا ادامه یابد. و با وجودی که تمرکـز سـازمان‌ها در ماه‌هـای اخیر بر نرم‌افزارهـای همـکاری و کنفرانس ویدیویی به‌عنـوان الزامـات کار از خانـه بوده اسـت، مطالعه‌ای که به تازگی از سـوی تحلیل‌گران مؤسسـهٔ گارتنر صورت گرفته نشان می‌دهد که شـرکت‌ها اکنون شـروع به فکـر کردن دربارهٔ بازگرداندن کارمندانشـان به محل کار کرده‌اند.
به گفتهٔ این تحلیل‌گـران، قطعاً انتظار تغییر وجـود دارد. و نـه تنها از سـوی کارمندان، بلکه از سـوی مدیران و گروه منابع انسـانی نیز. مطمئناً بسیاری از سازمان‌های بزرگ هم اکنون نگاه محافظه‌کارانه‌ای به این که آیندهٔ کار به چه شکلی درخواهد آمد انداخته‌اند.
نتیجـه ایـن مطالعـه نشـان می‌دهـد که دستیاران صوتی مانند کورتانا (مایکروسافت)، گوگل‌هوم یا الکسا (آمازون) که تاکنون جاذبهٔ کمی در محیط کار داشـتند، زیست‌سنجه‌ها (بیومتریـک) و حتـی نرم‌افزارهایـی کـه از هوش مصنوعی برای بازشناسی صدا استفاده می‌کننـد، می‌توانند نقش کلیـدی در تداوم فعّالیـت کسـب‌وکارها و در عین حال کمک به کارمندان در حفظ فاصلهٔ اجتماعی داشته باشند.
در اواسـط ماه مارچ، هنگامـی که کارمندان دفتری ناگهـان دریافتند که باید از خانه کار کنند، تعداد زیادی از سازمان‌ها متوجه شدند که برای در اختیار گذاشتن ابزارهای لازم به کارمندانشان آمادگی ندارند.
پس از اسـتفادهٔ گسـترده از رایانه‌های قابل حمـل، بُن‌سـازه‌های همـکاری و نرم‌افـزار کنفرانس ویدیویی، کسـب‌وکارها از سـه ماه پیش به دنبال مجوّز بازگشـایی برآمدند. این بـه معنی تغییر رویّه از سـرمایه‌گذاری برای ابزارهای کار از دور به فنّاوری مورد نیاز برای محیط کاری امن بود.
گـزارش گارتنـر پیش‌بینـی می‌کنـد کـه دسـتیاران صوتی و سـایر رابط‌هـای بدون تمـاس، بالاترین گزینه‌های سـرمایه‌گذاری بـرای سـازمان‌ها خواهنـد بـود و رابط‌های صوتـی کاربر، دسـتیاران هوشـمند و احراز هویّت زیست‌سـنجی نیز به‌طور گسـترده‌ای به‌کار گرفته خواهند شد.
قبـل از این بیماری دنیاگیر، به این قابلیّت‌ها به‌عنـوان ویژگی‌هایی که «داشـتنش خوب اسـت» نگاه می‌کردند. امّـا اگر فاصله‌گذاری اجتماعـی برای مدّتی طولانـی پابرجا بماند، ایـن فنّاوری‌ها برای هر شـرکتی که بخواهد کارمندانـش را بـه سـرکار بازگرداند، جنبهٔ حیاتی خواهند یافت.

آی‌تی ورلد، ۱۵ جون ۲۰۲۰

جلوگیـری آمـازون از اسـتفادهٔ پلیس از فنّاوری بازشناسی چهره

شـرکت آمازون اعلام کرد که به مدّت یکسال مانع اسـتفادهٔ پلیـس از فنّاوری بازشناسـی چهـره‌اش می‌گردد. این تصمیـم که به دلیل شـورش‌های اخیر رنگین‌پوسـتان در آمریکا گرفته شـده، نقطهٔ پایانـی خواهد بود بر یک جـدال دو سـاله بین آمـازون و فعّالان حوزهٔ آزادی‌های مدنی که نگرانـی خود را در مورد این کـه انطباق‌های نادقیق ممکن اسـت به دستگیری‌های ناروا بینجامد، اعلام کرده بودند.
مـرگ جورج فلوید، سیاهپوسـتی که در زیر زانوی افسـر پلیس سفیدپوسـت جـان داد، نگرانی‌ها را دربارهٔ استفادهٔ ناروا از بازشناسی چهره علیه تظاهرکنندگان افزایش داد.
بررسـی‌های پیشـین نشـان داده بـود که فنّـاوری آمـازون بـرای بازشناسـی چهـره (Rekognition) در تعیین جنسیّت افرادی با پوسـت تیره مشکل دارد. آمازون نتایج این بررسی را مورد تردید و اعتراض قرار داده بود. آمازون اعلام کرده اسـت که امیدوار است این ممنوعیّت یک ساله باعث شود تا کنگرهٔ آمریکا فرصت کافی برای تصویب قوانین مناسب در این

مورد داشته باشد. کنگره ماه‌هاست که سرگرم بحث در این مورد می‌باشد. در روزهای گذشته، آی‌بی‌ام اعلام کرد که دیگر فنّاوری بازشناسی چهره را عرضه نمی‌کند و مایکروسافت نیز فروش آن را متوقف کرده است.

به گفتهٔ رئیس اتحادیهٔ آزادی‌های مدنی در شمال کالیفرنیا، فنّاوری بازشناسی چهره به دولت‌ها قدرت بی‌سابقه‌ای برای جاسوسی از ما می‌دهد. او سایر شرکت‌ها را تشویق کرد که با پیوستن به مایکروسافت، آی‌بی‌ام، گوگل و آمازون، خود را در طرف درست تاریخ قرار دهند.

هنوز شرکت‌هایی مانند آیدمیا و اِن‌ای‌سی قراردادهای بزرگ‌تری با دولت برای بازشناسی چهره دارند. فروش Rekognition در سال ۲۰۱۸ معادل ۳ میلیون دلار از درآمد ۲۵/۷ میلیارد دلاری شرکت آمازون از خدمات ابری را تشکیل داده است.

رویترز، ۱۱ جون ۲۰۲۰

پایش فاصله‌گذاری اجتماعی و ماسک صورت با پهپاد

یک شرکت نوآفرین (استارتاپ) کالیفرنیایی به نام اِیراسپیس سیستمز که به تولید پهپاد می‌پردازد، نرم‌افزار جدیدی را برای پایش فاصله‌گذاری اجتماعی و پوشیدن ماسک صورت از هوا عرضه کرده است.

این نرم‌افزار فیلم‌های ویدیویی که توسط پهپادها گرفته شده را تحلیل می‌کند و می‌تواند تعیین کند که در کجا افراد به‌صورت خوشه‌ای در کنار یکدیگر قرار گرفته‌اند. این نرم‌افزار همچنین می‌تواند تشخیص دهد که افراد از ماسک صورت استفاده کرده‌اند یا نه. شرکت اِیراپیس سیستمز می‌خواهد نرم‌افزارش را به پلیس و مقامات شهرها بفروشد.

شرکت اِیراسپیس سیستمز اعلام کرده است که از بازشناسی چهره استفاده نمی‌کند و تصویر افراد را ذخیره نمی‌کند و به مشتریان نمی‌فروشد. به‌جای آن، داده‌هایی به‌صورت متنی تولید می‌کند که می‌گوید چند نفر در کجا اجتماع کرده بودند و چند درصد آن‌ها ماسک داشتند و بدین ترتیب، تولید هشدار می‌کند. مقامات شهر می‌توانند تصمیم بگیرند که این هشدارها را به‌صورت پیام‌های عمومی در اختیار ساکنان آن منطقه قرار دهند و یا آن را در اختیار پلیس برای برخورد قانونی و متفرّق کردن مردم قرار دهند.

با وجودی که سخنگوی شرکت اِیراسپیس سیستمز تأکید کرده که نرم‌افزار به ردگیری افراد نمی‌پردازد، امّا فعّالان حوزهٔ آزادی‌های مدنی این سامانه را گامی به سوی روبات‌هایی که رفتار ما را پایش می‌کنند می‌دانند.

رویترز، ۱۲ جون ۲۰۲۰

ممنوعیّت فروش بازشناسی چهره به پلیس از سوی مایکروسافت

شرکت مایکروسافت اعلام کرد که منتظر تصویب مقررات برای بازشناسی چهره از سوی کنگرهٔ آمریکا می‌ماند و تا آن زمان از فروش این فنّاوری به پلیس جلوگیری می‌کند. شرکت مایکروسافت آخرین شرکت بزرگی است که به دنبال تظاهرات سراسری در آمریکا در اعتراض به قتل یک سیاهپوست به دست پلیس، دست به این اقدام می‌زند.

این اعلان مایکروسافت کوتاه زمانی پس از آن صورت گرفت که شرکت آمازون هم اعلام کرد که استفادهٔ پلیس از فنّاوری بازشناسی چهره‌اش را متوقّف کرده است. مایکروسافت و آمازون هر دو اعلام نکرده‌اند که آیا این ممنوعیّت شامل سایر نهادهای قانونی مثل زندان‌ها هم می‌شود یا نه.

بنابر گزارش شرکت آی‌دی‌سی، این تصمیم شرکت‌های بزرگ، بیشتر جنبهٔ نمادین دارد و در حال حاضر بازشناسی چهره نقش چندانی در درآمد آن‌ها بازی نمی‌کند.

رویترز، ۱۱ جون ۲۰۲۰

مغزهای مصنوعی هم به خواب نیاز دارند

بر پایهٔ مطالعه‌ای که به تازگی در آزمایشگاه ملّی لوس‌آلاموس صورت گرفته است، شبکه‌های عصبی که پس از دوره‌های مداوم خودآموزی، ناپایدار می‌شوند دوباره پس از آن که در وضعیّتی شبیه خواب قرار گرفتند به حالت پایدار باز می‌گردند. در این مطالعه، ان دسته از شبکه‌های عصبی مورد بررسی قرار گرفتند که آموزش آن‌ها شبیه روش یادگیری انسان‌ها و سایر سامانه‌های زیست‌شناختی در دوران رشد کودکی از محیطشان است.

تیم پژوهشی آزمایشگاه لوس‌آلاموس دریافتند که شبیه‌سازی‌های شبکه پس از دوره‌های متوالی آموزش بدون نظارت، ناپایدار می‌شدند. پژوهشگران تصمیم گرفتند که شبکه‌ها را در معرض خواب مصنوعی قرار دهند. آن‌ها نوفه‌های گوناگونی را امتحان کردند، تقریباً شبیه آنچه که هنگام تنظیم امواج رادیو شنیده می‌شود. بهترین نتیجه هنگامی به‌دست آمد که آن‌ها از امواجی به نام نوفهٔ گاوسی که شامل محدودهٔ وسیعی از بسامدها و دامنه‌هاست استفاده کردند. آن‌ها چنین انگاشتند که نوفه، ورودی دریافت شده توسط نورون‌های زیست‌شناختی در هنگام خواب را تقلید می‌کند.

ساینس دیلی، ۸ جون ۲۰۲۰

رایانه‌هایی با ۱۰۰ برابر حافظهٔ بیشتر

پژوهشگران، مولکولی را کشف کرده‌اند که می‌تواند مانند ترانزیستور عمل کند و امکان ذخیره‌سازی اطلاعات دودویی را داشته باشد. اندازهٔ این مولکول در حدود ۵ نانومتر مربع است. یعنی بیش از یک میلیارد از آن‌ها بر روی یک تار موی انسان جای می‌گیرند. دانشمندان عقیده دارند که چنین مولکول‌هایی می‌توانند ۲۵۰ ترابایت اطلاعات را در یک اینچ مربع جای دهند که در حدود ۱۰۰ برابر گنجایش دیسک سخت‌های امروزی است.

با وجودی که پژوهشگران انتظار ندارند که مولکول‌هایی که کشف کرده‌اند در گرداننده‌های واقعی دیسک سخت به‌کار گرفته شود امّا مطالعهٔ آن‌ها اثبات مهم

مفهومی است که ما را به دنیای الکترونیک مولکولی نزدیک‌تر می‌سازد.
در این مطالعه، مولکول‌های یک نمک ارگانیک با استفاده از یک ورودی الکتریکی کوچک، روشن‌تر یا تیره‌تر به‌نظر می‌رسیدند- مشابه صفر و یک در رایانش امروزی. مهم‌تر آن که این اطلاعات قابل نوشتن، خواندن و پاک‌کردن در دمای اتاق و فشار هوای عادی است. این‌ها ویژگی‌های مهمی برای کاربرد عملی مولکول‌ها در دستگاه‌های حافظه است. اغلب پژوهش‌های پیشین دربارهٔ الکترونیک مولکولی برای کاربردهای مشابه، در خلأ و دماهای خیلی پایین صورت گرفته بود.

ساینس دیلی، ۲ جون ۲۰۲۰

جاوا هنوز برتر از پایتون و جاوا اسکریپت

جاوا، جاوا اسکریپت و پایتون در نمایه‌بندی‌های مختلف سه زبان برتر و محبوب‌تر برنامه‌نویسی هستند، هر چند ترتیبشان برحسب چگونگی رده‌بندی متفاوت است.
امّا یک بررسی جدید که توسط جت‌برین صورت گرفته نشان می‌دهد که جاوا که از نظر تاریخی محبوب‌ترین زبان برنامه‌نویسی است، هنوز بیشترین زبانی است که مورد استفادهٔ تولیدکنندگان نرم‌افزار می‌باشد.
این مطالعه نشان داد که محبوبیت پایتون به‌خاطر رشد یادگیری ماشین رو به افزایش است و این زبان، بیش از بقیهٔ زبان‌ها مورد مطالعه و آموزش قرار گرفته است. تقریباً یک سوم پاسخ‌دهندگان این بررسی گفته‌اند که ظرف سال گذشته شروع به آموزش یا ادامهٔ آموزش پایتون کرده‌اند.
استفاده از زبان تایپ اسکریپت مایکروسافت نیز رشد عمده‌ای داشته و اکنون زبان اوّلیه برای ۱۲٪ از تولیدکنندگان نرم‌افزار است. این نسبت در سال ۲۰۱۷ تنها یک درصد بود.
سه زبان برتری که تولیدکنندگان نرم‌افزار گفته‌اند که برای یادگیری آن‌ها برنامه‌ریزی کرده‌اند. زبان Go گوگل برای برنامه‌نویسی سیستم، زبان کاتلین که مورد پشتیبانی گوگل برای توسعهٔ اندروید می‌باشد و زبان پایتون بوده‌اند. زبان بعدی در این فهرست، زبان روست (Rust) است. این زبان توسط موزیلا برای برنامه‌نویسی سیستم ایجاد شده است. به دنبال روست، زبان‌های تایپ اسکریپت، سوئیفتِ اپل و دارتِ گوگل قرار دارند.
در میان تولیدکنندگان نرم‌افزار برای رایانه‌های رومیزی، ویندوز هدف اوّل است و به دنبال آن لینوکس و مک اواِس قرار دارند. رتبه‌بندی چهارچوب‌های چند بُن‌سازه‌ای تلفن‌های همراه نسبت به سال قبل تغییری نکرده و همچنان ری‌اکت نیتیو محبوب‌ترین بُن‌سازه (۴۲٪) و به دنبال آن فلوتر (۳۹٪) و آیونیک و کوردووا (۱۸٪) قرار دارند.

زد دی نت، ۱۶ جون ۲۰۲۰

راه‌حل‌های هوش مصنوعی هوآوی برای اروپا

هوش مصنوعی نقش اساسی در دگردیسی رقمی بازی می‌کند و در حال تغییر شکل دادن صنایع مختلف است. با در نظر گرفتن رشد سریع، همراه با انفجار باورنکردنی داده‌ها، انتظار می‌رود که هوش مصنوعی همانند ماشین بخار، دستگاه مولّد برق (ژنراتور) و روزنامه‌های چاپی، فنّاوری همه منظورهٔ دیگری باشد که تأثیر عمده‌ای بر زندگی انسان‌ها بگذارد. به عقیدهٔ تحلیل‌گران، هوش مصنوعی یکی از فنّاوری‌های مرکزی قرن بیست و یکم است و تأثیر بسیاری بر آیندهٔ زندگی بشر خواهد داشت.
به پیش‌بینی تحلیل‌گران، رایانش هوش مصنوعی تا سال ۲۰۲۵، نزدیک به ۸۰٪ کلّ بارکاری در مراکز رایانشی را به خود اختصاص خواهد داد. این میزان در حال حاضر کمتر از ۱۰٪ است. چنین رشد سریعی باعث شد تا شرکت هوآوی در سال ۲۰۱۹ معادل ۱۰۰ میلیون یورو در برنامه‌های پژوهشی هوش مصنوعی در اروپا سرمایه‌گذاری کند. این سرمایه‌گذاری ۵ ساله به کمک سازمان‌های صنعتی، ۲۰۰،۰۰۰ تولیدکنندهٔ نرم‌افزار و ۵۰ دانشگاه و مرکز پژوهشی برای پیش راندن نوآوری‌ها خواهد آمد.

نت‌ورک ورلد، ۶ می ۲۰۲۰

کاهش هزینه‌ها برای مقابله با زیان‌های ناشی از ویروس کرونا

بهبود وضعیت اقتصادی در دوران پساکرونا نیازمند آن است که مدیران عامل شرکت‌ها معیارهای کاهش هزینه‌ها را مورد ارزیابی جدّی قرار دهند.
تحلیل‌گران گارتنر توصیه می‌کنند که پیش از شروع هر پروژه‌ای در زمینهٔ بهینه‌سازی هزینه‌ها، نخست هیئت مدیرهٔ شرکت‌ها از آن پشتیبانی و برای سرمایه‌گذاری موافقت کنند.
گارتنر توصیه می‌کند که به هنگام ارزیابی هزینه‌ها، شش زمینه مورد توجّه و تمرکز مدیران عامل شرکت‌ها قرار گیرد.
۱- بررسی اندازه و درجه‌ای که پروژه‌های کاهش هزینه‌ها بر سود خالص شرکت تأثیر می‌گذارد.
۲- بررسی میزان صرفه‌جویی سازمان در صورت پیاده‌سازی اقدامات و چگونگی تأثیر آن بر جریان نقدینگی.
۳- تعیین تأثیر پروژه‌های کاهش هزینه‌ها بر روی کارکنان و عملیات روزمرهٔ کسب‌وکار، مانند بررسی تأثیر برکارایی و ارائهٔ محصول.
۴-تعیین بازهٔ زمانی مورد نیاز برای پیاده‌سازی و تداوم اقدامات مربوط.
۵- بررسی چگونگی یکپارچه‌شدن پروژه‌های کاهش هزینه‌ها با عملیات جاری و معماری سازمان.
۶- تعیین پروژه‌های حساس که ارزش تجاری دارند و حفاظت از استعدادهای کلیدی سازمان.

کامپیوتر ویکلی، ۱۵ جون ۲۰۲۰

تحلیل و مدل‌سازی امنیت در سیستم‌های اینترنت اشیاء (مروری بر چارچوب آپاراتوس)

فاطمه قربانی
دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات گرایش معماری سازمانی،
آزمایشگاه معماری سازمانی، دانشگاه صنعتی شیراز
پست الکترونیکی: f.ghorbani88@gmail.com

سیدرئوف خیامی
هیئت علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات،
آزمایشگاه معماری سازمانی، دانشگاه صنعتی شیراز
پست الکترونیکی: khayami@sutech.ac.ir

چکیده

سیستم‌های اینترنت اشیاء (IoT)، سیستم‌هایی پویا، مبتنی بر رویداد، در همه جا حاضر و به شدت پیچیده می‌باشند. این ویژگی‌ها باعث می‌شوند که تحلیل و بررسی این سیستم‌ها چالش برانگیز باشد. امنیت در IoT نیازمند ابزارها و متدولوژی‌های دامنه‌محور است. متدولوژی‌های پیشنهادی باید قادر باشند اطلاعات را از ساختارهای گوناگون، از ساختارهای نرم‌افزاری و سخت‌افزاری گرفته تا ساختارهای امنیتی و اجتماعی، جمع‌آوری کنند. در این مقاله، به معرفی یک چارچوب مدل‌سازی و تحلیل امنیت به نام آپاراتوس (APPARATUS) پرداخته می‌شود. آپاراتوس جهت تسهیل بررسی امنیت در سیستم‌های IoT توسعه داده شده است و علاوه بر مدل‌سازی در دو فاز طراحی و پیاده‌سازی یک نمادگذاری مبتنی بر کلاس برای زبان مدل‌سازی و یک رویکرد ساخت‌یافته برای گذار میان مدل‌های مختلف نیز پیشنهاد می‌کند. برای درک بهتر کاربرد این چارچوب، یک امنیت سیستم هوشمند حمل‌ونقل عمومی با استفاده از آپاراتوس مدل‌سازی و تحلیل امنیتی می‌شود. البته توسعه‌دهندگان این چارچوب برای تحلیل و بصری‌سازی امنیت سیستم، بخصوص در سیستم‌های مقیاس وسیع، یک ابزار تحت عنوان... نیز همراه با آن توسعه داده‌اند که بررسی آن خارج از حوزهٔ این نوشتار می‌باشد.

واژه‌های کلیدی: امنیت IoT، نیازمندی‌های امنیتی، امنیت شهرهای هوشمند، چارچوب آپاراتوس

۱- مقدمه

اینترنت اشیاء (IoT) از جمله حوزه‌های پژوهشی است که توجه قابل ملاحظه‌ای را معطوف خود کرده است. یکی از ویژگی‌های بنیادین سیستم‌های IoT ماهیت پویای این سیستم‌ها است، به این معنا که وضعیت دستگاه‌ها در طول چرخهٔ زندگی سیستم تغییر می‌کند. در شبکهٔ IoT، دستگاه‌ها برحسب اتصال و قطع اتصال، فعال و غیرفعال شدن پیوسته در حال تغییر وضعیت می‌باشند. از نقطه نظر امنیت این بدین معناست که در یک محیط عملیاتی به شدت پویا که نیازمندی‌های امنیتی، تهدیدات و آسیب‌پذیری‌های درحال تغییری دارد، تضمین اثربخشی کنترل امنیتی در طول زمان حائز اهمیت است.

شـهرهای هوشمند نمونه‌ای از کاربردهای پویا، پیچیده و مقیاس وسـیع از IoT هسـتند. کاربردهـای مختلف IoT در یک شـهر هوشـمند نیازمندی‌های امنیتی متفاوتـی دارند، با وجود این که نیازمندی‌های امنیتی از سـودبران مشابهی استخراج می‌شوند. از این رو مهندسـی سنتی نیازمندی‌های امنیتی و امنیت شبکه که از یک روش ایسـتا اسـتفاده می‌نماید برای چنین محیط پویایی کافـی نخواهد بود. بنابراین برای امن کردن یک سیسـتم IoT به ابزارها و سـازوکارهایی نیاز است که بتوانند با محیط خود تعامل داشـته و براساس تهدیدهای پیش رو امنیت خود را تغییر دهند. یکی از ابزارهای کارا در این حوزه اسـتفاده از مدل‌سازی مفهومی است.

چارچـوب آپاراتوس یـک چارچوب امنیتی بوده که در سـال ۲۰۱۸ توسعه داده شد و دارای بخش‌های زیر می‌باشد:

- یـک مدل مفهومـی برای نشـان دادن سیسـتم IoT در طول فاز طراحی. از مدل‌های فاز طراحی برای شناسـایی مولفه‌های امنیتی سـطح بالا، مثل سیاسـت های امنیتی و نیازمندی‌های سودبران، استفاده می‌شود.
- یک مدل مفهومی برای نمایش سیستم IoT در طول فاز پیاده‌سازی. این مدل برای شناسـایی و پیشنهاد کردن مولفه‌های امنیتی سطح پایین، مثل سازوکارهای امنیتی و آسیب‌پذیری‌های سیستم، قابل استفاده است.
- یـک رویکرد گام به گام بـرای حرکت میان مدل‌های فاز طراحی و پیاده‌سازی.
- نمادگذاری کلاس‌محور زبان مدل‌سازی چارچوب

۲- زبان مدل‌سازی آپاراتوس

یـک راه برای تحلیل امنیت سیسـتم‌های IoT اسـتفاده از مدل‌های سیسـتم‌های IoT اسـت. برای ایجـاد مدل نیاز به زبان مدل‌سـازی می‌باشـد. زبان مدل‌سازی از فرامدل‌هایی تشکیل شده است که برای نشـان دادن سیستم‌های IoT در لایه‌های مختلف مفاهیمی را تعریف می‌کنند.

یک سیسـتم IoT اساسا شـبکه‌ای از دسـتگاه‌های مختلف است، به همیـن دلیل مفاهیـم اصلی و اولیهٔ مدل مفهومی، دسـتگاه و اتصال شـبکه هستند. با استفاده از اطلاعات به دست آمده از معمار سیستم IoT و نیز نیازمندی‌های سودبران سیستم، نیازمندی‌های امنیتی قابل استخراج هستند.

مدل مفهومی آپاراتوس ماژولار است. مفاهیم زبان مدل‌سازی براساس زمینه موضوعیشان در ماژول‌های مختلفی دسته‌بندی می‌شوند. مزیت ایـن کار این اسـت که هر زمان تنها می‌تـوان از ماژول‌های موردنیاز استفاده نمود.

از آن جایـی که IoT دارای مولفه‌های شـبکه بندی کامپیوتر اسـت، مفاهیم شبکه‌های کامپیوتری، مثل اتصالات شبکه و دامنه‌های شبکه و نیـز مفاهیم زبان‌های مدل‌سـازی عمومی مثـل عامل (actor) در آپاراتوس ادغام می‌شوند.

مفاهیم نیازمندی‌های امنیتی که در این چارچوب مورد استفاده قرار می‌گیرند به روش نیازمندی‌های امنیتی Secure Tropos مدل‌سازی می‌شـوند. Secure Tropos به این دلیل انتخاب شـد که یک روش مهندسـی نیازمندی مستقر شده است که مفاهیم امنیتی آن با سایر روش‌های مهندسی نیازمندی‌ها هم راستاست.

یک نیازمندی امنیتی به این صورت تعریف می‌شود: یک قید مرتبط با موضوعات امنیتی مثل حریم خصوصی، یکپارچگی و دسترسی‌پذیری، که می‌تواند تحلیل و طراحی یک سیستم چندعامله تحت توسعه را با محدود کردن برخی از راه‌حل‌های طراحی جایگزین، تناقض داشـتن با برخی از نیازمندی‌های سیستم، یا با تصحیح کردن برخی از اهداف سیستم تحت تاثیر قرار دهد.

زبان مدل‌سازی از دو فرامدل تشکیل شده است. فرامدل اول مفاهیم و قیود مدل‌سازی یک سیستم IoT در طول فاز طراحی و فرامدل دوم مفاهیم و قیود مدل‌سـازی یک سیستم IoT در طول فاز پیاده‌سازی را ارائه می‌دهد.

در طول فاز طراحی، بدون در نظر گرفتن مشـخصات سخت‌افزاری یا نرم‌افزاری ایده سیستم مدل‌سازی می‌شود. به‌عنوان مثال ممکن است در طول فاز طراحی مشخص شود که به یک مولفه سیستمی به‌عنوان سیسـتم تشخیص نفوذ (IDS) نیاز است. اما ممکن است در این زمان مشخص نباشـد که این IDS یک دستگاه سخت‌افزاری خواهد بود یا یک برنامه نرم‌افزاری. در طول فاز پیاده‌سـازی مشـخص شـدن این موضـوع که IDS دسـتگاه سـخت‌افزاری خواهد بود یا یـک نرم‌افزار ضروری اسـت چرا که همبندی شبکه و نیازمندی‌های امنیتی آن را تحت تاثیر قرار می‌دهد.

اطلاعات مربوط به معماری سیستم را می‌توان در مدل‌سازی سیستم IoT گنجاند تا نتایج دقیق تری حاصل شود.

هـر فاز انواع مختلفی از تحلیل امنیتـی را ارائه می‌دهد. در طول فاز طراحی، تهدیدها و آسـیب‌پذیری‌های سیستم مدل می‌شوند. تحلیل امنیت در فاز طراحی نمی‌تواند برای نمایش آسـیب‌پذیری‌های خاص سیسـتم یا سـازوکارهای امنیتی کـه برای کاهش آن‌ها لازم اسـت استفاده شـوند. هم آسیب‌پذیری و هم سـازوکار امنیت مفاهیم یک سیسـتم پیاده‌سازی شده هسـتند چرا که نشان‌دهنده نقاط ضعف یا بهبود روی مولفه‌های سخت‌افزاری یا نرم‌افزاری سیستم هستند.

۲-۱- فرامدل فاز طراحی

فرامـدل فاز طراحی مجموعه قواعـدی را ارائه می‌دهد که ماژول‌های IoT فـاز طراحی باید به آن‌ها پایبند باشـند. ایـن فرامدل از طریق یـک نمـودار کلاس UML تعریـف می‌شـود. هـر کلاس UML به تعریـف یک مفهوم می‌پردازد، این مفهوم یا یک مولفه از سیسـتم را

توصیف می‌کند یا رفتاری که روی سیستم تاثیر می‌گذارد. مفاهیم از مجموعه‌ای از صفات (attribute) تشکیل شده‌اند که اطلاعات خاص مدل را ثبت می‌کنند. هر مفهوم دارای ویژگی description است که مولفه IoT سیستم را توصیف می‌کند، مگر این که خلافش قید شود. همان‌طور که در شکل ۱ نشان داده شده است، فرامدل فاز طراحی دارای مفاهیم زیر است:

۲-۱-۱- ماژول شبکه

۱- Device: شیئی از دنیای فیزیکی (شیء فیزیکی) یا یک شیء از دنیای مجازی (شیء مجازی) است. از این مولفه برای نشان دادن مولفه‌های فیزیکی، مثل محرک‌های سخت‌افزاری و گوشی‌های موبایل، یا مولفه‌های مجازی، مثل دستگاه‌های مبتنی بر ابر استفاده می‌شود.

۲- Application: بخشی از دنیای اطلاعات (شیء اطلاعاتی) است. یک برنامه کاربردی نمایشگر یک مولفه نرم‌افزاری است که روی یک Device اجرا می‌شود.

۳- Micronet: محیطی است که پیکربندی امنیت آن در اختیار معمار یا مهندس امنیت سیستم است. Micronet یک محیط مدیریت شده است، شامل مجموعه‌ای از دستگاه‌ها و برنامه‌های کاربردی که سیستم IoT را قادر می‌سازد کاری را به انجام برساند. خانه هوشمند مثالی از Micronet است. محدودهٔ Micronet در حین ایجاد مدل تعریف می‌شود. به‌عنوان مثال، یک Micronet می‌تواند تنها شامل دستگاه‌هایی باشد که بخشی از یک شبکه خاص هستند، در حالی که یک Micronet دیگر می‌تواند شامل تمام دستگاه‌های موجود در یک اتاق باشد. یک دستگاه می‌تواند به چند Micronet تعلق داشته باشد و هر Micronet می‌تواند کنترل‌های امنیتی مختلفی روی دستگاه‌ها اعمال کند.

purpose: هدف یا کارکرد Micronet را شرح می‌دهد.

۴- Net: نشان‌دهنده محیط‌هایی است که پیکربندی امنیتی آن‌ها ناشناخته است و رفتار آن‌ها قابل پیکربندی نیست. با وجود آن که ممکن است Netها مخرب نباشند اما نشان‌دهنده سطحی از خطر برای سیستم IoT می‌باشند که در طول توسعهٔ مدل باید موردتوجه قرار بگیرد. یک زیرساخت ابری نمونه‌ای از یک Net است که برای سیستم IoT شبکه خارجی محسوب شده و نسبت به امنیت آن دانش کمی وجود دارد یا اصلا دانشی وجود ندارد. این امکان وجود دارد که یک دستگاه بخشی از Net و یک Micronet باشد. به‌عنوان مثال، سیستم IoT کارسازی دارد که از مجموعه‌ای از ماشین‌های مجازی میزبانی می‌کند. با وجود آن که می‌توان کارساز را پیکربندی نمود، نحوهٔ استفاده از دارایی‌های مجازی کارسازها توسط کاربران پیکربندی می‌شود. در نتیجه دارایی‌های مجازی Net را تشکیل می‌دهند.

۵. Information: بیانگر داده‌های سخت، مانند لاگ‌های احرازهویت و داده‌های دمایی، یا داده‌های نرم، مانند اعتبارنامه‌های دسترسی و گذرواژه‌های کاربر است.

۲-۱-۲- ماژول اجتماعی

۱. actor: برای نشان دادن افراد یا گروه‌هایی از افراد است که با سیستم IoT تعامل دارند. actor می‌تواند یک سودبر سیستم باشد. actor ممکن است هیچ گاه مخرب نباشد.

intent: توصیف می‌کند actor می خواهد در تعامل با سیستم IoT به چیزی دست یابد.

۲-۱-۳- ماژول امنیتی

۱. Asset: هر application، device، actor یا information سیستم که (۱) از نظر سودبران ارزشمند بوده و نیاز به محافظت دارد، (۲) عامل مخرب به دنبال آن است، یا (۳) به‌عنوان یک جاپا برای حملات بعدی عمل می‌کند. در حالی که دارایی‌های ارزشمند سودبران در فاز نیازمندی‌ها قابل استخراج است اما دارایی‌هایی که مطلوب عامل مخرب بوده یا از آن‌ها می‌توان برای حملات بعدی استفاده کرد همیشه آشکار نیستند.

۲. Threat: یک کارکرد (تابع) که می‌تواند به‌صورت خرابکارانه به کار گرفته شود یا سیستمی که ابزار سوء استفاده از آسیب‌پذیری یک سیستم قانونی را در اختیار دارد. تهدید می‌تواند تنها یک دارایی از سیستم IoT را مورد هدف قرار دهد.

treatType: نشان‌دهندهٔ طبقه‌بندی تهدید (براساس STRID)

۳. Constraint: قیدی است مرتبط با موضوعات امنیتی چون حریم خصوصی، یکپارچگی و دسترسی‌پذیری، که می‌تواند از طریق محدود کردن برخی از راه‌حل‌های طراحی جایگزین، تناقض با برخی از نیازمندی‌های سیستم، یا با تصحیح برخی از اهداف سیستم روی تحلیل و طراحی یک سیستم تحت توسعه تاثیر داشته باشد. Constraint دارای ویژگی زیر می‌باشد:

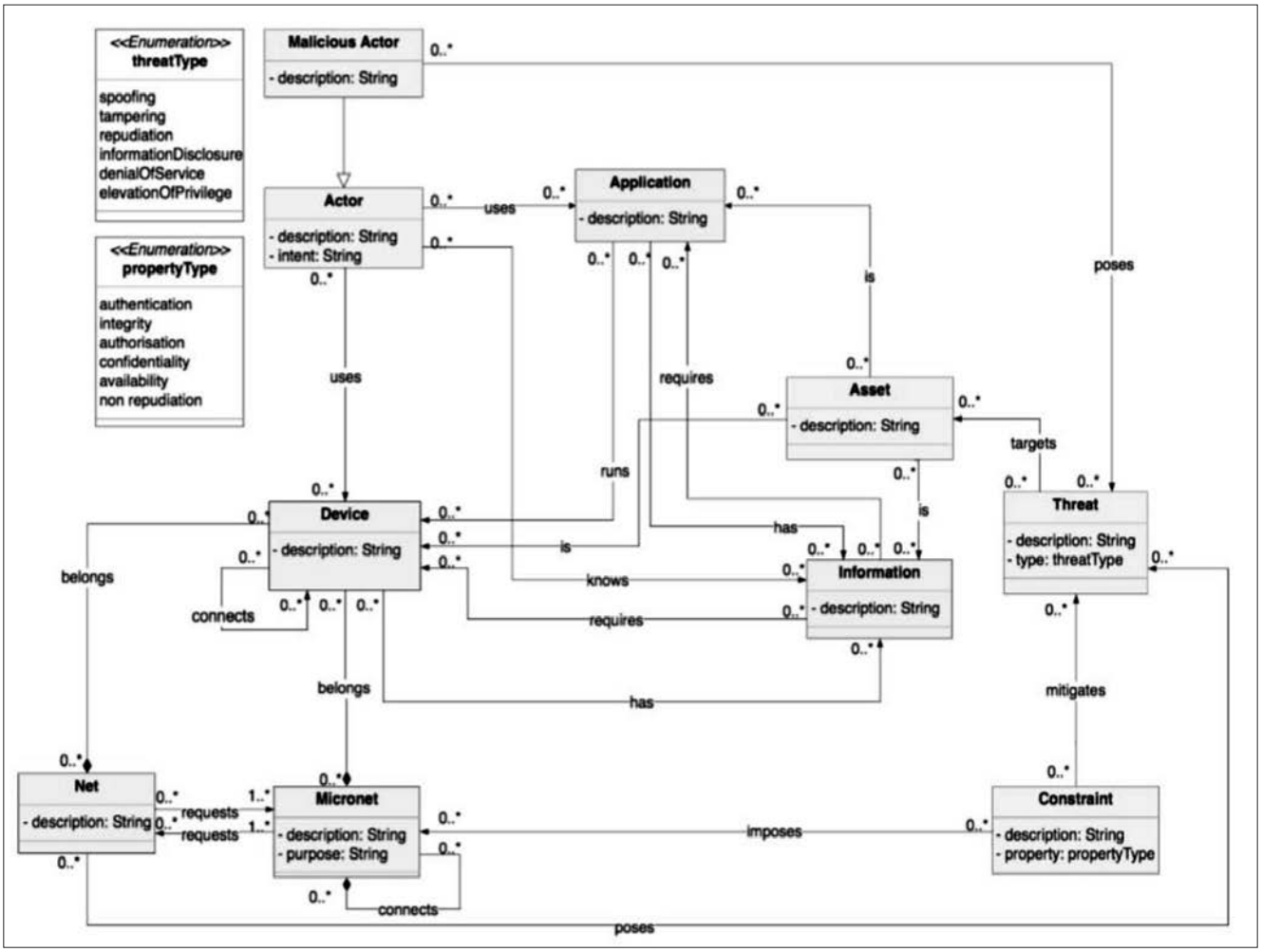
propertyType: طبقه‌بندی قید براساس سه گانه تعمیم داده شدهٔ CIA

۲-۲- فرامدل فاز پیاده‌سازی

فرامدل فاز پیاده‌سازی با مفاهیم و ویژگی‌های اضافی فاز طراحی را تصحیح می‌کند. مفاهیم و ویژگی‌های افزوده شده بیانگر اطلاعاتی هستند که در فاز طراحی ناشناخته بودند و برای تحلیل امنیت سودمند می‌باشند. به‌عنوان مثال در فاز طراحی نوع پروتکل‌هایی که در شبکه سیستم IoT مورد استفاده قرار می‌گیرند و نیز نسخهٔ نرم‌افزارهای دستگاه‌هایی که به سیستم سرویس می‌دهند مشخص نمی‌شود. از این اطلاعات اضافی می‌توان برای استخراج موضوعات امنیتی که در فاز طراحی آشکار نبودند استفاده نمود. فرامدل پیشنهادی در شکل ۲ نشان داده شده است.

مفاهیم اصلاح شده در فاز پیاده‌سازی عبارتند از: ۱) Device، ۲) Application، ۳) Micronet، و ۴) Information. مفاهیم اضافه شده شامل ۱) Vulnerabilityو ۲) Mechanism می‌باشد.

ماژول‌های فرامدل فاز پیاده‌سازی و مفاهیم آن به شرح زیر می‌باشد:



شکل ۱: فرامدل فاز طراحی

۲-۲-۱- ماژول شبکه

۱- Device: فـاز پیاده‌سـازی مفهوم Device در فـاز طراحی را با افزودن ویژگی‌هایی تصحیح می‌کند. ویژگی‌های اضافه شده Device عبارتند از:

- layer: لایه مفهومی در معماری IoT که دسـتگاه به آن تعلق دارد. آپاراتوس از یک معماری سـه لایه شامل لایه کاربرد، لایه شبکه و لایه ادراک استفاده می‌کند.

مقدار ویژگـی layer می‌تواند application (متناظر با لایه کاربرد)، gateway (متناظـر با لایه درگاه) یـا perception (متناظر با لایه ادراک) باشد.

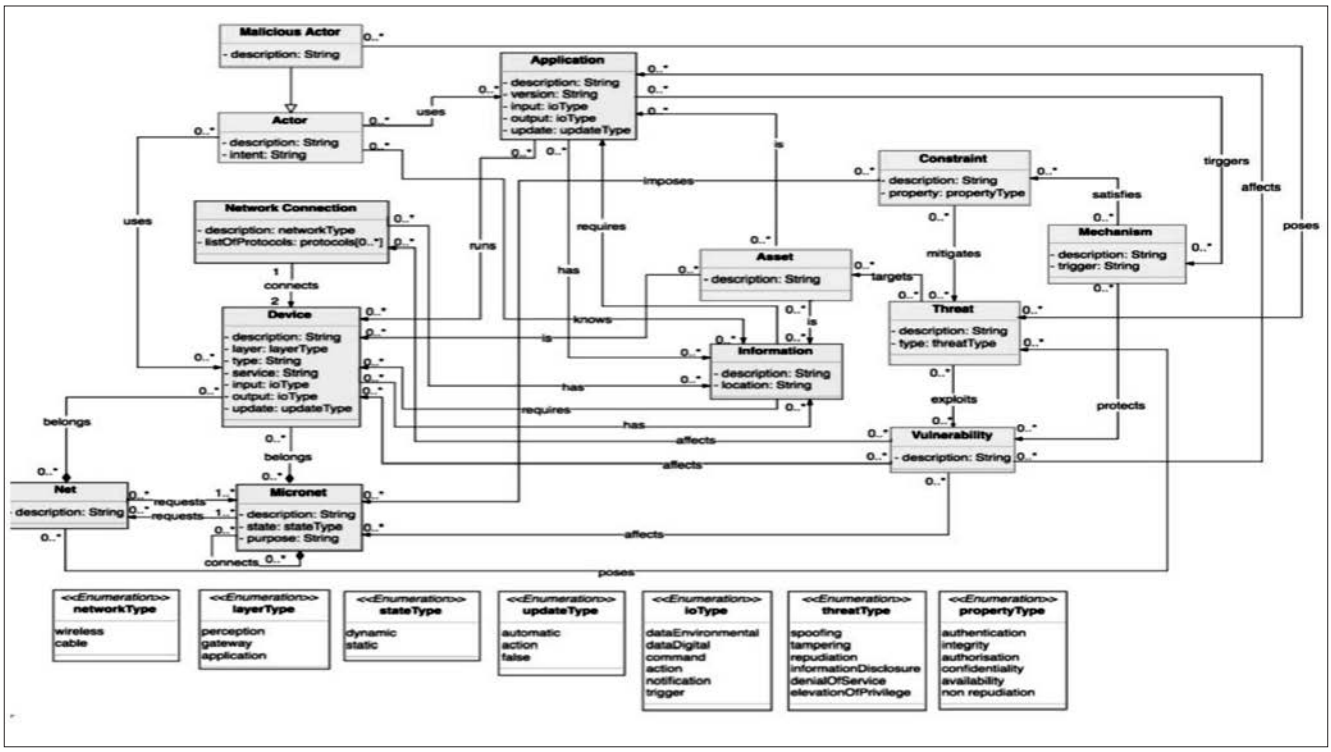
- type: برای تعریف نوع دستگاه استفاده می‌شود. مثلا یک دستگاه می‌تواند حسگر،گوشی موبایل یا یک کارساز باشد.
- service: نوع نقش یا عملیاتی است که دستگاه برای سیستم انجام می‌دهد. این مقدار می‌تواند شامل سرویس‌های شبکه (ftp، ssh)، فیلتر پردازش داده‌ها یا تقویت داده باشد.
- input: آنچـه که یک گره برای انجام نقـش یا عملیات خود بدان نیاز دارد. می‌تواند مقادیر، dataDigital، dataEnvironmental، trigger، notification، action، command را داشته باشد.
- output: نتیجـهٔ ایفای نقش یا انجام عمل دسـتگاه اسـت. همان مقادیر ویژگی input را می‌گیرد.
- update: نحوهٔ به‌روزرسـانی نرم‌افزار دسـتگاه را مشخص می‌کند. به‌روزرسانی می‌تواند خودکار بوده (automatic)، نیاز به یک عمل خاص داشته باشد (action) یا غیرفعال (false) باشد.

۲. Network Connection: نـوع پروتـکل ارتباطـی در شـبکه دستگاه‌ها را مشخص می‌سازد. ویژگی‌های Network Connection عبارتند از:

- description: نوع اتصال، می‌تواند wireless (اتصالی با استفاده از پروتکل بی سیم) یا cable (اتصال با استفاده از رسانه سیمی) باشد.

listOfProtocols: فهرستی از پروتکل‌هایی است که اتصال شبکه از آن‌ها پشتیبانی می‌کند. آرایه رشته‌ای را به‌عنوان ورودی می‌پذیرد که هر مقدار در این آرایه نشان‌دهنده یک پروتکل است.

۳- Application: فاز پیاده‌سازی مفهوم Application در فاز طراحی را بـا ویژگی‌هـای اضافی اصلاح می‌کند. ویژگی‌هـای Application عبارتند از:



شکل ۲: فرامدل فاز پیاده‌سازی

- version: شمارهٔ نسخهٔ نرم‌افزار.
- update: نحوهٔ به روزرسانی Application. به‌روزرسانی‌ها می‌توانند خودکار باشند (automatic) یا به اقدام خاصی نیاز داشته باشند (action) و یا غیرفعال (false) باشند.

۴- Micronet: فاز پیاده‌سازی مفهوم Micronet در فاز طراحی را با ویژگی‌های اضافی اصلاح می‌کند. ویژگی‌های Micronet عبارتند از:

state: ماهیت یک Micronet از لحاظ لایهٔ درگاه اتصال شبکه دستگاه. state می‌تواند dynamic (پویا، به این معنا که دستگاه‌های موجود در شبکه در طول استفاده دامنه‌های شبکه را تغییر می‌دهند، مثل هواپیماهای بدون سرنشین) یا static (ایستا، به این معنا که دستگاه‌های موجود در سیستم دامنه‌های شبکه را تغییر نمی‌دهند مثل خانه‌های هوشمند و سیستم‌های IoT صنعتی) باشد.

۵- Information: فاز پیاده‌سازی مفهوم Information در فاز طراحی را با اطلاعات اضافی تعمیم می‌دهد. ویژگی اضافی Information عبارت است از:

- location: متناظر با مکان جغرافیایی اطلاعات ذخیره شده در دستگاه می‌باشد. می‌توان از آن برای نمایش اطلاعاتی (داده‌ای) که به‌صورت فیزیکی درون شبکه ذخیره شده‌اند یا با یک سرویس شخص ثالث میزبانی می‌شوند استفاده نمود. علاوه بر این، نواحی مختلف قوانین متفاوتی دارند، نظر به این که اطلاعات دیجیتال در نهایت روی امنیت کل سیستم و قیود سیستم تاثیرگذار است.

۲-۲-۲- ماژول امنیت

۱- Vulnerability: یک نقطه ضعف در نرم‌افزار، سخت‌افزار یا کاربرد سیاست که می‌تواند توسط یک متخاصم علیه سیستم مورد بهره‌برداری قرار بگیرد. آسیب‌پذیری‌های نرم‌افزاری و سخت‌افزاری را می‌توان با دسترسی به پایگاه داده‌های آسیب‌پذیری (مثل CVE و NVD) شناسایی نمود. این پایگاه داده‌ها آسیب‌پذیری‌ها را با استفاده از شماره شناسایی منحصر به فرد ذخیره می‌کنند.

۲- Mechanism: در صورت اجرا از یک یا چند آسیب‌پذیری محافظت می‌کند. Mechanism می‌تواند به‌صورت خودکار و با تشخیص وقوع یک رویداد خاص توسط سیستم اعمال شود، یا می‌تواند فرآیندهای ثابت باشد.

- trigger: برای توصیف رفتار یا رویدادی که باعث به کارگیری Mechanism خواهد شد مورد استفاده قرار می‌گیرد.

در مدل‌سازی می‌توان ساختارهای مشابه مثل حوزه‌های حسگرها، کاربرانی با امتیازات یکسان یا نرم‌افزارهایی که پیکربندی یکسان دارند را یا با یک گره یا با گره‌های تکی نشان داد.

۳- نمادگذاری در آپاراتوس

مدل‌های چارچوب آپاراتوس به شکل گراف نشان داده می‌شوند. مفاهیم، گره‌های گراف و روابط میان گره‌ها یال‌های گراف را تشکیل می‌دهند. برخلاف سایر زبان‌های مدل‌سازی، که به شیوه‌ای ایستا و با استفاده از اشکال یا رنگ‌ها میان مفاهیم تمایز ایجاد می‌کنند، چارچوب آپاراتوس از کلاس‌ها استفاده می‌کند. دلیل استفاده از کلاس‌ها، جدا کردن نمایش تصویری از معنای واقعی مفاهیم است.

جدول۱: کلاس‌های نمادگذاری چارچوب آپاراتوس

رده	تعریف (definition)	توصیف (description)
normal	عنصر شرایط خاصی ندارد	با رنگ خاکستری کم رنگ یا مشکی نشان داده می‌شود
fade	نیاز به تمرکز روی عنصر نیست	با رنگ عنصر normal و با کاهش ۲۵ درصدی از تیرگی نشان داده می‌شود
first-selection	اولین عنصر انتخابی معمار یا مهندس امنیت است	با رنگ آبی نشان داده می‌شود
second-selection	دومین عنصر انتخابی معمار یا مهندس امنیت است	با رنگ نارنجی نشان داده می‌شود
attention	عنصر پیامدهای امنیتی دارد و نیازمند توجه می‌باشد	با رنگ نارنجی نشان داده می‌شود
protection	عنصر وضعیت امنیتی سیستم را بهبود می‌بخشد	با رنگ سبز نشان داده می‌شود

نمایش تصویری مدل‌های آپاراتوس متفاوت بوده و وابسته به نیازمندی‌ها و اولویت‌های مدل‌ساز می‌باشد. در آپاراتوس، نمایش تصویری با «چطور می‌خواهید مدل‌ها به نظر برسند» در ارتباط می‌باشد، در حالی که کلاس‌ها با آنچه «چه چیزی قرار است مورد توجه قرار بگیرد» مطابقت دارد.

از کلاس‌ها برای اضافه کردن ویژگی بصری یا متنی به عناصر گراف استفاده می‌شود. کلاس‌ها بسته به نوع اطلاعاتی که لازم است نشان داده شوند به‌صورت پویا روی گراف اعمال می‌شوند. به‌عنوان مثال فرض کنید هدف از تحلیل این است که مشخص شود آیا تمام تهدیدات در مدل کاهش داده شده‌اند یا خیر. برای تسهیل این نوع تحلیل، باید توجه روی عناصر مرتبط قرار گیرد و مابقی محو شوند. گره‌ها و یال‌های مرتبط با مفاهیم تهدید، قید و ارتباط کاهش است و باقی عناصر گراف مرتبط با موضوع تحلیل نیستند. ASTo (ابزاری که آپاراتوس از آن برای ساده کردن تحلیل سیستم‌های بزرگ استفاده می‌نماید و اساس کار آن نمادگذاری مبتنی بر کلاس است) از الگوریتم زیر برای اعمال خودکار کلاس‌ها استفاده می‌کند:

- کلاس fade روی تمام عناصر موجود در گراف اعمال می‌شوند.
- کلاس attention روی تمام مفاهیم تهدید اعمال می‌شوند.
- کلاس protection روی تمام مفاهیم محدودیت اعمال می‌شود.
- کلاس normal روی تمام روابط کاهش اعمال می‌شود.

هر کلاس یک definition و یک description دارد. definition اطلاعاتی که ما می‌خواهیم در یک زمان خاص به تحلیل‌گر منتقل کنیم را بیان می‌کند. description ویژگی‌های متنی و بصری که به عنصر اضافه شده‌اند را نشان می‌دهد. در حالی که تعریف کلاس‌ها قابل تغییر نیست، توصیف را می‌توان اصلاح نمود، چرا که توصیف کلاس‌ها به نمایش مرحلهٔ پیشین[1] مدل‌ها ارجاع دارد و از این رو می‌تواند قابل تغییر باشد. به‌عنوان مثال یک مجموعه از توصیفات کلاس می‌تواند مولفه‌های بصری را به گره‌ها اضافه کند، مثل رنگ‌ها یا اشکال، در حالی که مجموعه دیگری می‌تواند مولفه های متنی، مثل برچسب‌ها، را اضافه کند. جدول ۱ کلاس‌های نمادگذاری چارچوب آپاراتوس را نشان می‌دهد. چارچوب آپاراتوس روش خاصی را برای نمایش تصویری مدل‌ها تحمیل نمی‌کند.

۴- قواعد گذار میان فازهای مهندسی مختلف

در صورتی که لازم باشد مدل‌های سیستم در هر دو فاز طراحی و پیاده‌سازی ایجاد شوند می‌توان از مدل موجود برای فاز طراحی برای گذار به فاز پیاده‌سازی استفاده کرد و بالعکس و به این ترتیب فرآیند توسعه را کوتاه کرد.

با وجود این که جریان کاری معمول مهندسی سیستم از فاز طراحی به فاز پیاده‌سازی است، اما ممکن است شرایطی به وجود بیاید که معمار یا مهندس سیستم مجبور باشد از فاز پیاده‌سازی به فاز طراحی برود. توسعهٔ مجدد یک سیستم IoT موجود نمونه‌ای از این شرایط است. در این حالت اگر مدل فاز پیاده‌سازی وجود داشته باشد فرآیند گذار به فاز طراحی مقرون به صرفه نخواهد بود. در چارچوب آپاراتوس معمار سیستم می‌تواند سیستم IoT موجود را با مدل فاز پیاده‌سازی مدل‌سازی نموده سپس با استفاده از قواعد گذار از پیاده‌سازی به طراحی، فاز طراحی سیستم را تولید کند. برای تسهیل فرآیند گذار میان دو فاز مهندسی، یک رویکرد ساخت یافته تعریف شده است که از آن می‌توان برای گذار میان فازهای مختلف (طراحی به پیاده‌سازی و برعکس) استفاده نمود.

۴-۱- قواعد گذار از فاز طراحی به فاز پیاده‌سازی

۱- به مفاهیم Micronet ویژگی state داده می‌شود.

۲- به مفاهیم Device ویژگی‌های، input، service، layer،type، update، output داده می‌شود.

۳- مفهوم طراحی Device که با سایر Devices ها ارتباط connect دارد، با مفهوم Network Connection جایگزین می‌شود.

۴- به مفاهیم Application ویژگی‌های update، version داده می‌شود.

۵- به مفاهیم Information ویژگی location داده می‌شود.

۶- سایر مفاهیم بدون تغییر باقی می مانند.

۴-۲- قواعد گذار از پیاده‌سازی به طراحی

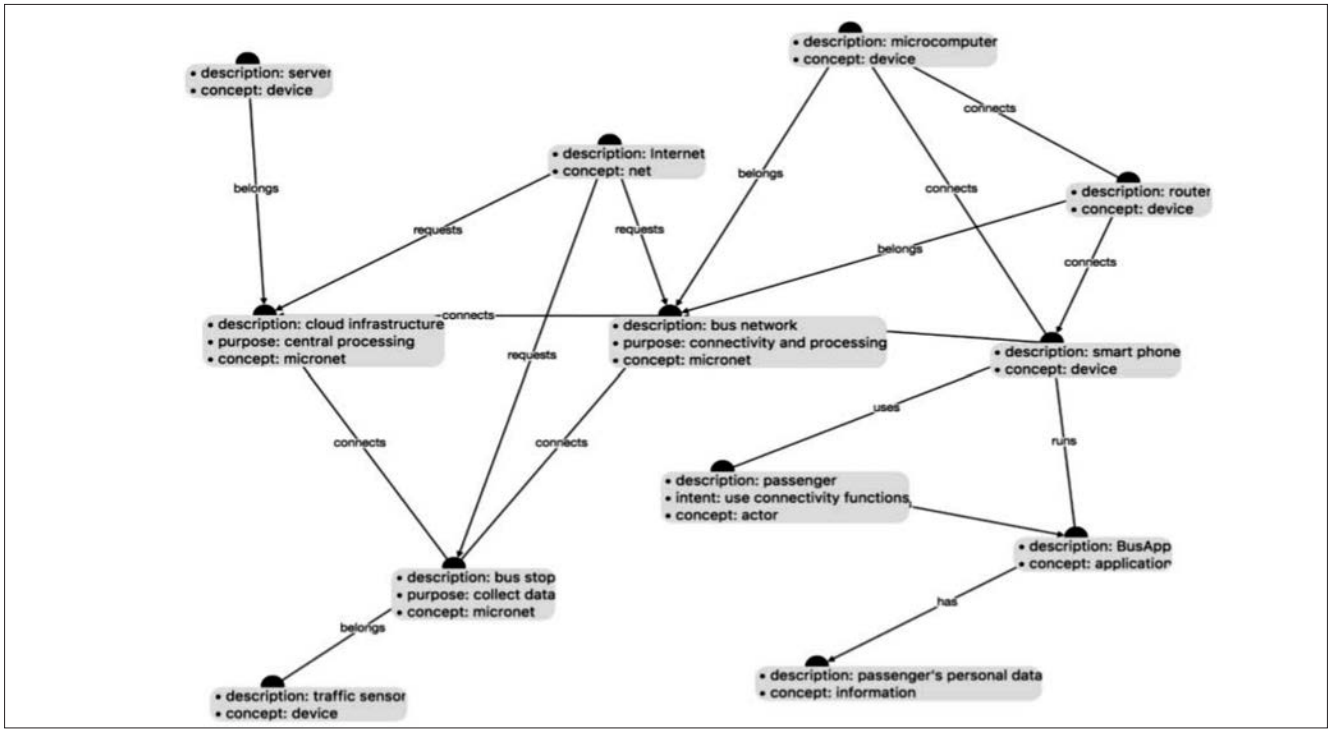
۱- ویژگی‌هایی که در گام‌های فوق تعیین شدند از مفاهیم حذف می‌شوند.

۲- مفاهیم Mechanism حذف می‌شوند.

۳- مفاهیم Vulnerability حذف می‌شوند.

۵- مثالی از تحلیل امنیت با استفاده از چارچوب آپاراتوس

1- front-end



شکل ۳: مدل شبکه و اجتماعی سیستم در فاز طراحی

برای نشـان دادن نحوهٔ بـه کارگیری چارچـوب آپاراتوس در تحلیل امنیت، یک تحلیل امنیتی جزئی روی سیسـتم هوشمند حمل‌ونقل عمومی انجام می‌دهیم. این سیستم نشان‌دهنده یک سیستم هوشمند حمل‌ونقـل عمومـی در دنیای واقعی نیسـت و تنهـا زیرمجموعه‌ای از ایـن سیسـتم فرضی تحلیل و مدل‌سـازی می‌شـود. در این مثال تحلیل امنیتی از فاز طراحی شـروع می‌شـود. مولفه‌های نرم‌افزاری و سخت‌افزاری سیستم عبارتند از:

۱- یک واحد پردازشـگر مرکزی که به‌عنوان نقطـه کانونی پردازش برای کل سیستم عمل می‌کند.

۲- یک میکروکامپیوتر روی بورد اتوبوس. این میکروکامپیوتر به‌عنوان یک واحد پردازشگر برای عملیات داخلی اتوبوس عمل می‌کند.

۳- یک مسـیریاب روی بورد اتوبوس. مسیریاب از طریق اتصال LTE، شبکه وای فای موردنیاز برای اتصال مسافران و سایر بخش‌های شبکه به سیستم اتوبوس را تامین می‌کند.

۴- حسـگرهای هوشـمند روی ایسـتگاه‌های اتوبوس. این حسگرها اطلاعات ترافیک و مسیر را میان اتوبوس‌ها و واحد پردازشگر مرکزی مبادله می‌کنند.

۵- گوشی‌های هوشمند مسافران که از برنامه موبایل سیستم هوشمند حمل‌ونقل عمومی استفاده می‌کنند.

سودبران سیستم در این مثال کاربران سیستم حمل‌ونقل هستند. همان‌طور که در شـکل ۳ نشـان داده شده اسـت، می‌توان براساس مولفه‌های سیسـتم و با اسـتفاده از ماژول‌های اجتماعی و شبکه در چارچوب آپاراتوس، مدل فاز طراحی را ایجاد نمود.

حمل‌ونقل عمومی هوشمند دارای نیازمندی‌های امنیتی زیر است که از سودبران به دست آمده:

SR1: مسـافران نباید قادر به دسـتکاری سیسـتم‌های سخت‌افزاری اتوبوس باشند.

SR2: نبایـد از طریـق منابع اتوبـوس امکان دسترسـی غیرمجاز به داده‌های شخصی مسافران وجود داشته باشد.

ایـن نیازمندی‌ها هسـتهٔ تحلیل امنیتی را تشـکیل می‌دهند. از این نیازمندی‌هـا برای شناسـایی تهدیدات، قیود و دارایی‌های سیسـتم استفاده می‌شود.

تحلیل امنیتی در آپاراتوس متمرکز بر دارایی است. بنابراین اولین گام، شناسـایی دارایی‌های سیستم است. براساس SR1 و SR2 دارایی‌های زیر در سیستم شناسایی می‌شوند:

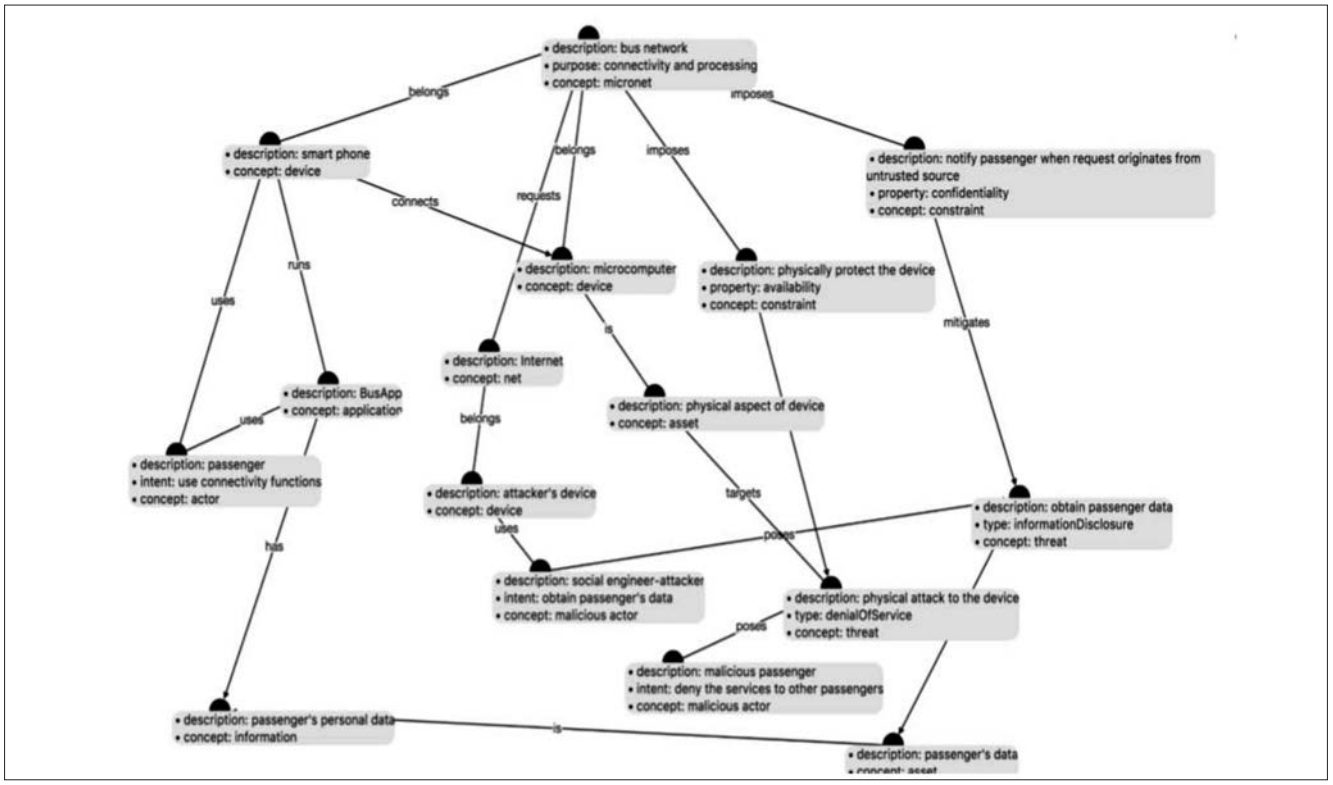
A1: جنبه فیزیکی ریزکامپیوتر اتوبوس

A2: اطلاعات شخصی مسافران

دومین گام در تحلیل امنیت، مدل‌سـازی تهدیدات سیستم براساس دارایی‌های شناسایی شده است.

T1: حملـه فیزیکی به ریزکامپیوتر برای انجام حمله DoS. این تهدید روی دارایی A1 تاثیر می‌گذارد و از یک مسافر با مقاصد مخرب نشئت می‌گیرد. حمله کننده به‌صورت فیزیکی به دسـتگاه آسـیب می‌زند و به این ترتیب منابع دسـتگاه برای کاربران قانونی غیرقابل دسـترس می‌شوند.

T2: بـه کارگیری برنامه حمل‌ونقل هوشـمند برای به دسـت آوردن اطلاعات شـخصی مسافران از طریق مهندسـی اجتماعی. این تهدید



شکل ۴: مدل سیستم Micronet اتوبوس در فاز طراحی

A2 را تحت تاثیر قرار می‌دهد. حملهٔ ناشی از این تهدید از اتصالات خارجی (در این مثال اینترنت) نشئت می‌گیرد.

بعد از مدل‌سازی تهدید نوبت به قیود سیستم می‌رسد. قیود زیر برای کاهش تهدیدات شناسایی شده (T1 و T2) پیشنهاد می‌شوند:

C1: محافظت فیزیکی ریزکامپیوتر برای کاهش T1

C2: برنامه حمل‌ونقل هوشمند باید هر زمان که از یک منبع ناشناخته درخواستی مبنی بر دسترسی به اطلاعات شخصی یک مسافر رسید آن را به اطلاع مسافر برساند.

مدل سیستم Micronet که نسخه نهایی تحلیل امنیت است در شکل ۴ نشان داده شده است.

با پایان یافتن تحلیل امنیتی در فاز طراحی، گام بعدی انجام تحلیل امنیتی در فاز پیاده‌سازی است. به این منظور از اعمال کردن قواعد گذار از فاز طراحی به پیاده‌سازی استفاده می‌شود.

در فاز پیاده‌سازی تعدادی از مولفه‌ها مثل Application، Device و Micronet ویژگی‌های اضافی دریافت می‌کنند تا اطلاعات دقیق را بهتر نشان دهند. این ویژگی‌ها با استفاده از اطلاعات به دست آمده از سودبران سیستم تعیین می‌شوند.

بعد از اعمال قواعد گذار و گرفتن اطلاعات لازم از سودبران، مدل سیستم در فاز پیاده‌سازی (شکل ۵) ایجاد می‌شود.

فاز پیاده‌سازی دو مولفه اضافه‌تر از فاز طراحی دارد تا وضعیت امنیتی سیستم را بهتر نشان دهد و این دو مؤلفه عبارتند از Mechanism و Vulnerability.

V1: دسترسی فیزیکی به دستگاه (ریزکامپیوتر) برای عامل‌ها و عامل‌های مخرب یکسان است (T1).

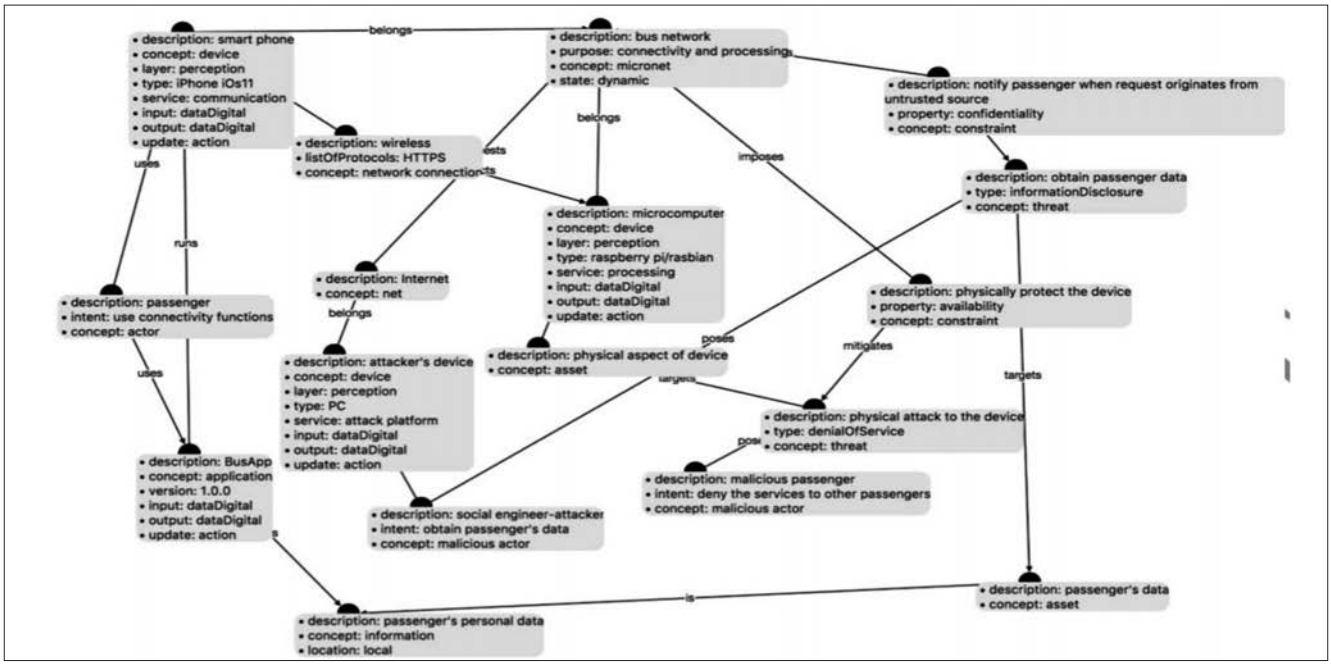
برای محافظت سیستم در برابر V1 پیشنهاد می‌شود که ریزکامپیوتر در یک مکان امن قرار بگیرد (M1).

V2: براساس اطلاعات به دست آمده از سودبران، نرم‌افزار سیستم هوشمند درخواست‌ها را براساس مبدا درخواست پاکسازی نمی‌کند. این بدین معناست که رفتار یکسانی با تمام درخواست‌ها می‌شود، چه از منبع قابل اعتماد باشند چه از منبع غیرقابل اعتماد (T2).

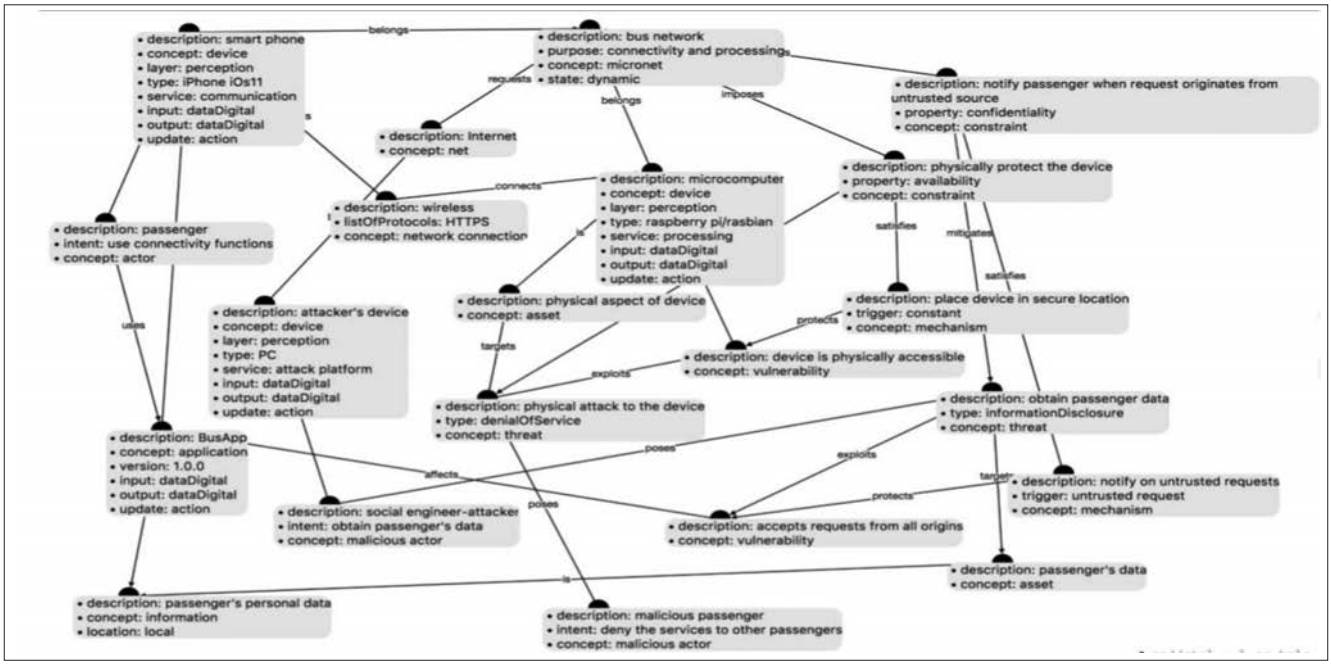
برای مقابله با این آسیب‌پذیری پیشنهاد می‌شود که درخواست دسترسی به داده‌های شخصی مسافران به اطلاع آن‌ها رسیده و آن‌ها بتوانند درخواست‌های منبع غیرمعتبر را به‌صورت دستی قبول یا رد کنند (M2).

V3: مولفه‌های نرم‌افزاری و سخت‌افزاری سیستم ویژگی update با مقدار action دارند. Action نیازمند این است که عامل به‌صورت دستی به روزرسانی را روی دستگاه یا نرم‌افزار انجام دهد. و این به این معناست که وقتی بهره‌برداری جدیدی از یک مولفه خاص کشف شود سیستم تا زمانی که عامل به روزرسانی را انجام دهد در معرض خطر خواهد بود.

بسته به شدت بهره‌برداری، در سیستم سازوکاری قرار داده شود که تا زمان به روزرسانی با مولفه‌های قابل بهره‌برداری مانند دستگاه‌های در معرض خطر قرار گرفته رفتار کند(M3).



شکل ۵: مدل سیستم Micronet اتوبوس در فاز پیاده‌سازی با اعمال قواعد گذار روی مدل فاز طراحی



شکل ۶: مدل امنیتی سیستم Micronet اتوبوس در فاز پیاده‌سازی

مدل سیستم پیاده‌سازی که شامل نسخه نهایی تحلیل امنیت است در شکل ۶ نشان داده شده است.

۶- محدودیت های چارچوب آپاراتوس

محدودیت این چارچوب این است که برای ایجاد مدل‌ها نیازمند تخصص خاص دامنه (دانش نسبت به معماری شبکه، دارایی‌های سیستم و نیز تعاملات میان سیســتم و کاربر) است. ایجاد فرایندهای خودکار و نیمه خودکار برای مدل‌سازی به‌عنوان کار آینده پیشنهاد می‌شود.

منبع

Mavropoulos, O., Mouratidis, H., Fish, A., Panaousis,E.: Apparatus: A Framework for Security Analysis in Internet of Things Systems (2018). Ad Hoc Networks

مدل بلوغ تعامل‌پذیری کشور*

هانیه کشفی
دانشجوی دکتری، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران
پست الکترونیکی: h_kashfi@sbu.ac.ir

حسن حقیقی
دانشیار، دانشکده مهندسی و علوم کامپیوتر، دانشگاه شهید بهشتی، تهران
پست الکترونیکی: h_haghighi@sbu.ac.ir

مازیار مباشری
دفتر تدوین ضوابط فنی و مقررات دولت الکترونیکی، سازمان فناوری اطلاعات ایران، تهران
پست الکترونیکی: mobasheri@ito.gov.ir

امیرحسین محیط
دفتر تدوین ضوابط فنی و مقررات دولت الکترونیکی، سازمان فناوری اطلاعات ایران، تهران
پست الکترونیکی: mohit@ito.gov.ir

چکیده

در این مقاله، مدل بلوغ تعامل‌پذیری کشور به اختصار معرفی شده‌است. عناصر اصلی مطرح در این مدل شامل سطوح بلوغ، ابعاد مورد بررسی، شاخص‌های ارزیابی و همچنین روش ارزیابی سطح بلوغ تعامل‌پذیری است. این مدل دارای ده سطح بلوغ به‌همراه شش بُعد جهت بررسی تعامل‌پذیری است. جهت بهبود کیفیت ارزیابی، ابعاد به شاخص‌هایی ملموس و قابل اندازه‌گیری در سازمان‌ها/سیستم‌های اطلاعاتی تجزیه شده است که هر یک از این شاخص‌ها در سطوح مختلف امتیازاتی را در زمینه تعامل‌پذیری به خود اختصاص می‌دهند. در نهایت با امتیازدهی به شاخص‌ها، امکان تعیین سطح بلوغ تعامل‌پذیری برای یک سازمان وجود خواهد داشت. بر مدل ارائه شده، نحوه ارزیابی تعامل‌پذیری از سه جنبهٔ بلوغ تعامل‌پذیری بین دو سیستم اطلاعاتی/سازمان، بلوغ تعامل‌پذیری در یک سیستم اطلاعاتی و بلوغ تعامل‌پذیری در یک سازمان بیان خواهد شد.

واژه‌های کلیدی: تعامل‌پذیری؛ مدل بلوغ تعامل‌پذیری؛ شاخص‌های تعامل‌پذیری؛ سطوح تعامل‌پذیری؛ ابعاد تعامل‌پذیری.

۱- مقدمه

با جهانی شدن روزافزون کسب‌وکارها و افزایش تعاملات ناگزیر در سازمان‌های کشور، امکان ایجاد همکاری‌های مختلف جهت تبادلات محصولات، سرویس‌ها و اطلاعات در داخل و خارج سازمان‌ها ضروری

* این مقاله در سومین همایش ملی پیشرفت‌های معماری سازمانی، ۲۲ و ۲۳ آبان ۱۳۹۸ ارائه شده است.

اســت. در بســیاری موارد حتی از هر دو سمت ســودبران و مشتریان ســازمان (به‌عنوان مثــال در زنجیره تامیــن) تلاش‌های جدی جهت بهبود تعامل‌پذیری در ســازمان‌ها در حال انجام است. در کشور ایران نیز با وجود ســرعت تغییرات بازار و تکامل سیستم‌های موجود، ارائهٔ راهکارهایی به‌روز برای این امر ضروری می‌نماید. البته تعابیر متفاوتی از مفهوم تعامل‌پذیری در ســازمان‌ها مطرح اســت که در این مطالعه تعریف تعامل‌پذیری ســازمانی ارائه شــده توسط INTEROP در سال ۲۰۰۷ مبنای کار قرار گرفته است [۱]. طبق این تعریف تعامل‌پذیری سازمانی به‌عنوان ظرفیت یک نرم‌افزار یا برنامه کاربردی برای برقراری تعامل با سایر نرم‌افزارها معرفی می‌شود.

بر اســاس مطالعات CMMI، اســتفاده از مدل بلــوغ تعامل‌پذیری در سازمان‌ها شــش مزیت عمده را برای سازمان به همراه خواهد داشت [۲]:

• ســازگاری: با وجود مدل بلوغ تعامل‌پذیری و تعیین سطح بلوغ در ســازمان‌ها، میزان ســازگاری و انطباق مورد انتظار بین دو ســازمان تعامل‌پذیر قابل پیش‌بینی خواهد بود.

• صرفه‌جویی در هزینه‌ها: با اســتفاده از این مدل و نیز ســطح بلوغ تعامل‌پذیری در ســازمان‌ها، هزینه‌های دوباره‌کاری و ایجاد تغییرات در برنامه‌ریزی‌ها کاهش یافته و شــرایط مناســبی بــرای پیش‌بینی هزینه‌های مصرفی فراهم می‌شود.

• خود-بهبودی: با ارزیابی تعامل‌پذیری ســازمان توســط این مدل و تعیین ســطح بلوغ آن، سازمان با اطلاع از ســطح بلوغ تعامل‌پذیری خود، به ارتقای ســطح خود توسط نقشــه‌راه تعبیه شده توسط مدل تشویق می‌شود.

• حرکت مبتنی بر تقاضای بازار: ســازمان با اطــلاع از تقاضای بازار همزمان با آگاهی از سطح بلوغ خود، می‌تواند سطوح بلوغ لازم جهت برآورده کردن نیازمندی‌های مشــتریان را شناسایی کرده و به سمت آن حرکت کند.

• حرکــت مبتنی بر کارایــی لازم: مدل بلــوغ تعامل‌پذیری با تعیین نقــاط ضعف و قوت هر ســازمان در برقراری تعامــل، فرصت خوبی جهــت شناســایی نقاط ضعف و رســیدن بــه کارایــی لازم را ایجاد می‌کند.

• بهبود فرآیند: تعیین ســطح بلوغ تعامل‌پذیری در ســازمان فرصت مناســبی را جهت استانداردســازی فرآیندها و تــلاش برای انطباق با به‌روش‌ها در این حوزه فراهم می‌سازد.

در ایــن مقاله مدل بلــوغ تعامل‌پذیری جدیدی با الگــو برداری از ۲ مــدل بلوغ مشــهور [۳، ۴] و نشــئت گرفته از معماری ســرویس‌گرا ارائه شــده اســت. یکی از دلایل اســتفاده از منظر ســرویس‌گرایی و معماری ســرویس‌گرا در بررســی ســطوح بلوغ تعامل‌پذیری، رویکرد دولــت الکترونیکــی به ســمت معمــاری ســازمانی ســرویس‌گرا و مباحث ســرویس‌گرایی اســت. دلیل عمده دیگر این است که امروزه جهت‌گیری‌های اغلب ســازمان‌ها نیز به همین ســمت است. نوآوری دیگر مقاله در ارتباط با روش ارزیابی متناســب با شاخص‌های مطرح در ابعاد مختلف مدل بلوغ است.

ســایر بخش‌های مقاله دارای ســاختار ذیل است. در بخش ۲ به مرور مدل‌های بلوغ ارائه شــده در زمینه تعامل‌پذیری پرداخته شده است. در بخش ۳، مدل بلوغ تعامل‌پذیری کشــور و عناصر آن معرفی شــده است و در نهایت بخش ۴ حاوی نتیجه‌گیری مقاله است.

۲- مــرور مدل‌هــای بلــوغ ارائــه شــده در زمینــه تعامل‌پذیری

در ایــن بخش به‌طور مختصــر به مرور مدل‌های بلــوغ تعامل‌پذیری مطرح پرداخته می‌شود.

۲-۱- مدل بلوغ تعامل‌پذیری OSIMM

مدل بلوغ یکپارچگی معماری سازمانی یا OSIMM[1] یکی از مدل‌های استانداردی است که به سازمان‌ها برای رسیدن به یک مدل کسب‌وکار سرویس‌محور یاری می‌رساند و با ارائه این مدل سعی دارد ابزاری را در اختیار سازمان‌ها قرار دهد که بتوانند به واسطه آن نقشه راه پیشرفت خود را در زمینه سرویس‌ها و سیستم‌های اطلاعاتی مشخص نمایند. به‌عبارت دیگر استفاده از این چارچوب به سازمان‌ها کمک می‌کند تا به‌شــکل تکاملی و گام به‌گام به سمت دستیابی به سطوح بالغ‌تر بلوغ یکپارچگی سرویس‌ها دســت یابد تا به‌واسطه آن ارزش‌های بیشتری برای کســب‌وکار ایجاد شــود. مدل بلوغ OSIMM برای تعیین سطح بلوغ یکپارچگی ســرویس‌ها، هفت بُعد شامل کســب‌وکار، سازمان و حاکمیت، روش‌ها و متدها، برنامه‌های کاربردی، معماری، اطلاعات و مدیریت زیرساخت را مورد بررسی قرار می‌دهد و بر این اساس آن‌ها می‌توانند در هفت ســطح بلوغ شامل ســیلو، یکپارچه‌شده، مولفه‌ای، سرویس، ســرویس‌های مرکب، ســرویس‌های مجازی‌شــده، قابلیت پیکربندی پویا قرار گیرند [۳].

۲-۲- مدل بلوغ تعامل‌پذیری CSOAMM

براســاس [۴]، مــدل بلــوغ CSOAMM[2] ترکیبــی از مــدل بلــوغ تعامل‌پذیــری OSIMM و مــدل بلــوغ ســرویس‌گرایی SOAMM اســت. این مدل شــامل ده ســطح ســیلو، یکپارچه، مولفه‌ها، آزمون فنی، وب‌ســرویس اولیه، نهادینه‌سازی، ســرویس‌های معماری‌شده، سرویس‌های داخلی و خارجی، سرویس‌های اندازه‌گیری شده، قابلیت پیکره‌بندی سرویس‌های پویا است. همچنین ابعاد مطرح در این مدل بلوغ مطابق با ابعاد موجود در مدل OSIMM است.

۲-۳- مدل بلوغ تعامل‌پذیری LISI

مدل بلوغ LISI[3] نشان‌دهنده سطح تعاملات میان سیستم‌های اطلاعاتی

1-Open group Service Integration Maturity Model

2- Combined Service Oriented Architecture Maturity Model

3- Levels of Information Systems Interoperability

می‌باشـد. در مدل LISI پنج سـطح بلوغ مختلف شامل تعامل‌پذیری منزوی در یک محیط دسـتی، تعامل‌پذیـری متصل در یک محیط نظیر بـه نظیر، تعامل‌پذیـری کارکردی در یک محیط توزیع‌شـده، تعامل‌پذیـری دامنـه محور در یـک محیط یکپارچـه، تعامل‌پذیری سـازمان محور در یک محیط فراگیر، معرفی شده‌اند. مدل LISI ابعاد مختلف تعامل‌پذیری یک سیستم اطلاعاتی را در چهار دسته اصلی رو یه‌ها، برنامه کاربردی، زیرساخت و داده قرار می‌دهد [۵].

۲-۴- مدل بلوغ Interoperability Potential

نـوآوری اصلـی مطرح در ایـن مدل بلـوغ، ارائـه معیارهایی جهت اندازه‌گیری میزان تعامل‌پذیری در ابعاد مختلف است. این مدل شامل پنج سـطح بلوغ ایزوله، اولیه، اجرایی، متصل و تعامل‌پذیر است. ابعاد مطرح نیز در این مدل شـامل موارد کسب‌وکار، فرآیند، منابع انسانی، دانش سازمانی، ICT و معنای مطرح در سازمان است [۶].

۲-۵- مدل بلوغ تعامل‌پذیری OIMM[4]

این مدل بلوغ شامل سـطوح یکپارچه، ترکیبی، مشارکتی، موردی و مسـتقل است که با سطوح مطرح در LISI همراستا هستند. همچنین در هر سطح ۴ بعد مختلف مورد بررسی قرار گرفته است. در حالی که هدف درکارهای پیشین بررسی تعامل‌پذیری در سطح سیستم و فنی اسـت، این مطالعه مسایل مرتبط با تعامل‌پذیری در سطح سازمان را بررسـی می‌کند. البته در این مدل روش و معیاری جهت اندازه‌گیری تعامل‌پذیری ارائه نشده‌است [۷].

۲-۶- مدل بلوغ تعامل‌پذیری EIMM

ایـن مدل بلوغ پنج سـطح مختلف از قابلیت‌های تعامل‌پذیری شـامل انجام شده، مدل‌سازی شده، یکپارچه، تعامل‌پذیر و بهینه شده را تعریف می‌کند. این مدل سطوح بلوغ سازمان را با توجه به استفاده از مدل‌های سـازمانی و توانمندی این مدل‌ها در امکان ایجاد همکاری برای سازمان ارزیابی می‌کند. بر اساس ارزیابی‌های این مدل سازمان‌ها به سمت انتخاب مفاهیم بهتر جهت ایجاد تعاملات با در نظر گرفتن توانمندی‌هایشـان و همچنین شـرایط محیط و چالش‌های آن راهنمایی می‌شوند. همچنین این مدل شـامل چهار بعد کسـب‌وکار، فرآیند، سرویس و داده است. در این مدل نیز پارامترها و روش‌های خاص و واضحی برای بررسـی بلوغ و پیش‌روی در مسیر آن مشخص نشده است [۸].

۲-۷- مدل بلوغ تعامل‌پذیری Knight

ایـن مدل بلوغ دارای پنج سـطح از قابلیت‌های تعامل‌پذیری شـامل سطوح اولیه، مدیریت شده، تعریف شده، مدیریت شده به‌صورت کمی و بهینه شده است و ابعاد مطرح در این مدل نیز در ۶ دسته پیکربندی و تحول، امنیت و ایمنی، عملیات و کارایی، سـاختاری و اطلاعاتی و فنی قرار می‌گیرند. این مدل بلوغ در سـال ۲۰۱۷ ارائه شده و در آن معیارهایی جهت ارزیابی سـطوح بلوغ تعامل‌پذیری سازمان نیز برای ابعاد مختلف مطرح است [۲].

۲-۸- مدل بلوغ تعامل‌پذیری ISIMM[5]

مدل بلوغ تعامل‌پذیری سیسـتم‌های اطلاعاتی در سـال ۲۰۱۲ ارائه شـده است. این مدل پنج سـطح بلوغ مختلف شامل دستی، موردی، همکارانه، یکپارچه و متحد شده را معرفی می‌کند. همچنین چهار بعد مختلف در این مدل ارائه شـده‌اند که عبارتنـد از بعد داده، نرم‌افزار، ارتباطات و فیزیکی. لازم به ذکر اسـت که این مدل شامل معیارهای ارائه شده در سطوح و ابعاد مختلف بوده و در نهایت یک روش ارزیابی سطح بلوغ تعامل‌پذیری را ارائه می‌دهد [۹].

۲-۹- مدل بلوغ تعامل‌پذیری پیشین کشور

این مدل بلوغ تعامل‌پذیری در سـال‌های ۹۳-۹۴ توسـط پژوهشکده سیاسـت‌گذاری و مدیریت راهبردی فاوا – گروه توسعه کسب‌وکار و کارآفرینی ارائه شـد. هفت سطح بلوغ این مدل شامل سطوح منفرد، متصل، مبتنی بر مولفه، مبتنی بر سرویس، مبتنی بر سرویس مرکب، مبتنی بر سـرویس مجازی و مبتنی بر سـرویس پویا است. پنج بعد تعامل‌پذیری نیز شـامل نرم‌افزار، زیرسـاخت فیزیکـی، پروتکل‌های ارتباطی، اطلاعات و فرآیند برای این مدل مطرح شـده‌اند. البته مدل ارائه شده شامل معیارهایی برای هر بعد بوده و در نتیجه روشی برای ارزیابی نیز ارائه می‌دهد [۱۰].

۳-مدل بلوغ تعامل‌پذیری کشور

مدل بلوغ تعامل‌پذیری پیشـین کشور بر مبنای مدل بلوغ OSIMM بوده کـه هم‌اکنون با توجه بـه معماری سـرویس‌گرای جاافتاده در سـازمان‌ها، مدل چندان جامعی نیسـت. لذا مدل بلوغ تعامل‌پذیری جدید کشـور با تاکید بر مفهوم معماری سـرویس‌گرا ارائه شده و بر مبنای مدل SOAMM مورد بازبینی قرار گرفته اسـت. تعداد سطوح در مدل پیشین هفت سطح بود که در مدل جدید به ده مورد افزایش پیدا کرده اسـت. و البته اسامی سـطوح با هدف سفارشی‌سازی برای نیازمندی‌های کشور ایران، تغییراتی داشته است. ابعاد مطرح در مدل پیشـین پنج مورد بود که در مدل جدیـد در نتیجه ادغام دو مورد از ابعاد مدل پیشـین و افزودن دو بعد جدید، تعداد ابعاد در مدل جدید به شـش مورد افزایش یافت. همچنین شـاخص‌های مطرح در مدل پیشـین دوازده مورد بود که بر اسـاس مطالعات اخیر در مدل جدید جهت ایجاد سـهولت در ارزیابی سطح بلوغ تعامل‌پذیری سازمان‌ها به بیست‌وپنج مورد افزایش یافت.

۳-۱- چارچوب مدل بلوغ تعامل‌پذیری کشور

در مدل بلوغ تعامل‌پذیری کشـور، ده سطح بلوغ مجزا در نظر گرفته

4- Organizational Interoperability Maturity Model

5- Information Systems Interoperability Maturity Model

شده است که می‌توانند به دستگاهی که بررسی می‌شود، نسبت داده شوند. این سطوح ده‌گانه بلوغ عبارتند از:

۱. سطح یک (منفرد): در سطح اول با عنوان «منفرد»، سیستم‌های اطلاعاتی به‌شکل مجزا و منفرد مشغول به فعالیت هستند و نهایتا یکپارچه‌سازی در سطح داده وجود دارد. در این سطح وجود سیلوهایی از برنامه‌های کامپیوتری محض با عملیات متمرکز و غیرقابل دسترس معمول است. همچنین در این سطح قابلیت‌های زیرساختی برای برقراری تعاملات و ارتباطات میان سیستم‌ها مهیا نیست و تنها در صورت مداخله انسانی و با استفاده از ابزار کاغذی یا رسانه‌های قابل‌حمل و جداشدنی امکان برقراری ارتباط و تعامل میان سیستم‌ها وجود دارد.

۲. سطح دو (یکپارچگی محدود): در سطح دو با عنوان «یکپارچگی محدود»، سیستم‌ها قادر هستند به شکل محدود به هم متصل شوند و تا حدودی یکپارچه‌سازی در سطح برنامه کاربردی وجود دارد. در این سطح، با وجود مهیا بودن زیرساخت فیزیکی برای تعاملات، برقراری تعاملات و ارتباطات میان سیستم‌ها با پیچیدگی بالایی همراه است. در این شرایط ممکن است سیستم‌ها به‌شکل نیمه‌مکانیزه و با مشارکت انسان و ابزارهای برخط نظیر رایانامه، رجوع به وبگاه‌ها و...، با یکدیگر تعامل داشته باشند. این سطح را می‌توان شکلی از یکپارچه‌سازی برنامه کاربردی سازمان (EAI) در نظر گرفت. جریان اطلاعات در این سطح، از طریق رویکردهای پیام‌گرای EAI، هماهنگ می‌شود. سازمان از روش‌های ساخت‌یافته به سمت روش‌های شیءگرا و همچنین از معماری یکپارچه به سمت معماری لایه‌ای حرکت کرده است. با این حال هنوز هم در این سطح برخی اتصالات موردی و نقاط یکپارچه‌سازی نظیر به نظیر وجود دارد.

۳. سطح سه (مبتنی بر مولفه): در سطح سه با عنوان «مبتنی بر مؤلفه»، مولفه‌ها شناسایی شده و عملکردها به صورت ماژولار وجود دارند. ارتباطات در این سطح بر اساس قراردادها و واسط‌ها است. در این سطح از تعامل‌پذیری، سیستم‌های اطلاعاتی به مؤلفه‌های کارکردی مختلفی شکسته می‌شوند. واسط‌های این مؤلفه‌ها در اختیار سیستم‌های اطلاعاتی دیگر قرار می‌گیرند و از این طریق، برقراری ارتباطات و تعاملات را تسهیل می‌کنند. نکته‌ای که می‌بایست مورد اشاره قرار گیرد اینست که در این سطح از تعامل‌پذیری، همچنان میان مؤلفه‌های کارکردی وابستگی‌های زیادی وجود دارد و از این رو، برقراری ارتباط و تعامل میان سیستم‌ها برای پیاده‌سازی فرآیندهای میان‌سیستمی امری پیچیده و دشوار است.

۴. سطح چهار (حرکت به سمت سرویس‌گرایی): در سطح چهارم با عنوان «حرکت به سمت سرویس‌گرایی»، عمده سرویس‌ها شناسایی و تعریف شده‌اند و برخی از سرویس‌ها نیز طراحی شده‌اند؛ این سطح از بلوغ سرآغاز مشاهده نشانه‌هایی از سرویس‌گرایی می‌باشد. در این سطح سرویس‌ها دارای وابستگی سست با یکدیگر می‌باشند؛ همچنین مفاهیمی مانند وب‌سرویس در این سطح معرفی می‌شوند. در این سطح، ارائه سرویس‌ها قطعی شده است و فرهنگ سازمانی به سمت پذیرش نظم سرویس‌گرایی در حرکت است. همچنین در این سطح یکپارچگی با سیستم‌های موروثی و نوسازی این سیستم‌ها وجود دارد.

۵. سطح پنج (مبتنی بر سرویس): در سطح پنجم، با عنوان «مبتنی بر سرویس»، عمده سرویس‌ها شناسایی، تعریف، طراحی و پیاده‌سازی شده و حتی استقرار و انتشار یافته‌اند و سازمان یک دید سرویس‌گرا از فناوری اطلاعات دارد؛ معماری سرویس‌گرا با متدولوژی‌های توسعه یکپارچه شده و کدها و پروتکل‌های اختصاصی و موردی با سرویس‌ها جایگزین شده‌اند. این اولین سطحی است که از معماری سرویس‌گرا برای تامین نیازهای ضروری سازمانی استفاده شده است؛ عملکردهای جدیدی تعریف شده‌اند؛ فرآیندها با استفاده از تعامل‌های مبتنی بر توصیف سرویس یکپارچه شده‌اند. همچنین یک ثبت سرویس جهت ایجاد بخش فنی معماری به کار گرفته شده است.

۶. سطح شش (نهادینه شدن معماری سرویس‌گرا): سطح ششم تحت عنوان «نهادینه شدن معماری سرویس‌گرا» مطرح است. در این سطح، معماری سرویس‌گرا با فرآیند توسعه در سراسر سازمان یکپارچه شده است. همچنین معماری سرویس‌گرا در این سطح از طریق آموزش در سازمان نهادینه شده و عملکردهای سازمان با سرویس‌ها یکپارچه شده است. در نهایت، تعاریف سرویس‌ها در مخزن سرویس ذخیره شده است. همچنین همنواسازی[6] و هم‌آرایی[7] سرویس‌ها نیز تا سطح بالایی انجام شده است.

۷. سطح هفتم (پنجره واحد ارائه خدمات): سطح هفتم تحت عنوان «پنجره واحد ارائه خدمات» مطرح است. در این سطح از بلوغ تعامل‌پذیری، ارائه یک سرویس مستلزم تعامل سرویس‌های دیگر نیز می‌باشد که سرویس‌گیرنده الزاماً از آن‌ها و تعاملات میان آن‌ها آگاه نخواهد بود. در این سطح، کنترل معماری سرویس‌گرا افزایش یافته است و علاوه‌براین، یک معماری دقیق از چندین برنامه کاربردی یکپارچه و یک SSO بر روی این برنامه‌های کاربردی ایجاد شده است.

۸. سطح هشتم (مبتنی بر سرویس مرکب): سطح هشتم با عنوان «مبتنی بر سرویس مرکب» مطرح است. در این سطح از بلوغ تعامل‌پذیری، ارائه یک سرویس مستلزم تعامل سرویس‌های دیگر نیز می‌باشد که سرویس‌گیرنده الزاماً از آن‌ها و تعاملات میان آن‌ها آگاه نخواهد بود. در این سطح، شکاف بین فناوری اطلاعات و کسب‌وکار به‌طرز محسوسی کاهش یافته و تمامی

6- Orchestration
7- Choreography

عملکردهای کسب‌وکار به سرویس‌ها متصل هستند و در نتیجه می‌توان گفت یک یکپارچگی کامل بین عملکردهای کسب‌وکار وجـود دارد. درواقـع در این سـطح هیچ تفاوتـی بین مدیریت فرآیند کسـب‌وکار و مدیریت فرآیند سـرویس وجود ندارد. این سـطح آخرین مرحلـه از تحولات فناوری اطلاعات در سـازمان اسـت که منجر به سـرویس‌های ترکیبی می‌شود. سرویس‌های ترکیبی توسـط سـرویس هم‌نواساز مدیریت می‌شـوند. اتصال بین سـرویس‌های داخلی و خارجی، امکان گسترش فرآیندهای کسب‌وکار به سازمان‌های خارجی را میسر می‌سازد؛ و در نتیجه می‌توان کل زنجیره تامین را یکپارچه کرد.

۹. سـطح نهم (مبتنی بر سـرویس مجازی): سـطح نهم با عنوان «مبتنـی بر سـرویس مجازی» مطرح اسـت. پس از گسـترش فرآیندهای کسب‌وکار به سـازمان‌های خارجی، باید کسب‌وکار را از حالـت انفعالی به یک کسـب‌وکار زمان-واقعی تبدیل کرد. جهت نیل به این هدف، جداسازی سرویس از برنامه‌های کاربردی زیرساختی و نهایتا ایجاد سرویس‌های مجازی ضروری است. در این سـطح از بلوغ ارائه سـرویس‌ها و همچنیـن تعاملات میان آن‌ها به‌شـکل مستقل از بستر و زیرسـاخت، انجام می‌شود. در این سـطح ممکن‌است مفاهیم و فناوری‌هایی نظیر ESB و GSB مطرح شوند که بدون وجود ارتباطات مستقیم و دو به دو، امکان برقراری تعامل در سرویس‌ها را فرآهم می‌آورند. در چنین حالتی تغییرات احتمالی مورد نیاز به‌صورت تبدیل نشـانی‌ها، شـبکه، قراردادها، اسـتانداردهای اطلاعاتی و ...، به‌صورت خودکار انجام می‌شوند و برای انجام این تبدیلات نیاز به منابع انسانی نمی‌باشد و از این رو انعطاف‌پذیری بالایی به‌چشـم می‌خورد. این معماری در واقع مبتنی بر یک زیرسـاخت تورین[8] و مسـتقل از فناوری اسـت. در نتیجه تنظیم مناسـب زیرسـاخت و تغییر مدل‌های کسـب‌وکار قدیمی و یا حتی ایجاد مدل‌های کسب‌وکاری جدید ضروری اسـت. علاوه‌برایـن، ارزیابی و بازمهندسـی فرآیندهای کسـب‌وکار در حال اجرا نیز مهم است. تمام این موارد از طریق تحلیل فرآیندهای کسـب‌وکار جهت تعریـف معیارهای کارایی مبتنی بر کسب‌وکار انجام می‌شود. اندازه‌گیری کارایی به صورت زمان-واقعی به وسـیله سـرویس پایش فعالیت‌های کسب‌وکار میسـر می‌گـردد. در این سـطح، مدیریت، پایـش، و مدیریت رخداد در معماری توسـط سـرویس‌های مجزا انجام می‌شـود. همچنین سـرویس‌های تبدیل در گذرگاه سـرویس سازمانی یا گذرگاه خدمات دولت به پشـتیبانی از ناهمگونی و توزیع‌شدگی سیستم‌ها کمک می‌کنند.

۱۰. سـطح ده (مبتنـی بـر سـرویس پویـا): در سـطح دهم تحت عنوان «مبتنی بر سـرویس پویا»، یک معماری پویا بر اسـاس سرویس‌های مرکب ایجاد شـده در زمان اجرا مطرح است. یک معماری مبتنی بر رخداد که به صورت خودکار قابل بازپیکربندی است، فرآیندهای کسب‌وکار خودکار را مدیریت می‌کند. در این سـطح می‌توان معماری سـرویس‌گرا را به‌عنوان سیستم عصبی سـازمان با مفاهیـم حس و پاسـخ پویا معرفی کرد کـه نهایتا منجر به یک سـازمان خود-سازمانده می‌شـود. در این سطح از تعامل‌پذیری، سـرویس‌ها و تعاملات مورد نیاز برای ارائه آن‌ها با بالاترین سطح از انعطاف‌پذیری و سرعت ارائه خواهند شد.

در ادامه این بخش به معرفی ابعاد ارزیابی تعامل‌پذیری به‌عنوان یکی از مهمترین مؤلفه‌های شـکل دهنده مدل بلوغ تعامل‌پذیری پرداخته خواهد شـد. در نسخه جدید مدل بلوغ تعامل‌پذیری کشور شش بُعد تعامل‌پذیری در نظر گرفته شـده اسـت که هر یک به‌نحوی بر روی تعامـلات اثرگذار خواهند بود. در ادامه این بخش، به معرفی این ابعاد شش‌گانه پرداخته می‌شود:

- زیرساخت: یکی از ابعادی که در زمینه بلوغ تعامل‌پذیری اهمیت بالایی دارد، زیرسـاخت تعاملات می‌باشـد. به وضوح مشـخص اسـت در صورتی که زیرساخت مناسـب برای برقراری تعاملات فراهم نباشـد (حتی در صـورت آمادگی ابعاد دیگـر)، برقراری تعامل میان سیستم‌ها/سـازمان‌ها میسـر نخواهد بود. سازگاری بُن‌سازه‌های فناوری اطلاعات و همچنین استفاده از قراردادهای ارتباطی سازگار بین شرکا از جمله دغدغه‌هایی است که بایستی در بعد زیرسـاخت مورد بررسی قرار گیرد. منظور از قراردادهای ارتباطی، استانداردها و مشـخصه‌هایی هستند که در حوزه‌های مختلـف، به انتقال بهتر اطلاعات به‌منظـور برقراری بهتر تعامل میان سیسـتم‌ها کمک می‌کنند. این اسـتانداردها و مشخصه‌ها در قالب فهرسـتی با عنوان فهرست استاندارد فنی، در چارچوب تعامل‌پذیری کشور معرفی شده‌اند.
- داده و اطلاعات: یکی از عوامل مهمی که می‌بایسـت در مبحث تعامل‌پذیـری مورد توجه قـرار گیرد، مبحـث داده و اطلاعات اسـت، زیرا داده و اطلاعـات در تعاملات، مبادله شـده و باعث گـردش بهتر فرآیندها برای ارائه خدمات می‌شـود. اهمیت این موارد در تعامل‌پذیری به حدی است که معمولاً در چارچوب‌های تعامل‌پذیری کشـورهای مختلف سـرفصلی برای تعامل‌پذیری اطلاعاتـی (معنایی) وجود دارد که فهرسـت اسـتاندارد داده و شِـماهای XML معرف آن است. بر این اساس، میزان استاندارد بودن داده و اطلاعاتی که می‌بایسـت در تعاملات مبادله شـوند، یکی از عوامل اثرگذار بر روی بلوغ تعامل‌پذیری می‌باشد. در این بعد از تعامل‌پذیری، سـازمان به دنبال این اسـت که، مدل‌های داده‌ای مختلـف بـا یکدیگـر کار کننـد. تعامل‌پذیـری داده و اطلاعـات مربوط به یافتن داده و اطلاعات مشـترکی اسـت که از منابـع مختلـف و ناهمگون تولید می‌شـوند و می‌توانند روی ماشـین‌های متفاوتی با سیسـتم‌عامل‌ها و سیستم‌های مدیریت پایگاه داده مختلف و ناهمگون نیز مستقر شوند.

8- Grid

- برنامه کاربردی: یکی از مهمترین مؤلفه‌های اثرگذار بر روی بلوغ تعامل‌پذیری، قابلیت‌های نرم‌افزاری است. سیستم‌های اطلاعاتی در ارائه خدمات مختلف دولتی نقش دارند و می‌توان عنوان کرد تعاملاتی که می‌بایست در خلال ارائه خدمات دولت الکترونیکی ارائه شوند، در واقع تعاملات میان سیستم‌های اطلاعاتی مرتبط با خدمات می‌باشند. از این رو یکی از مهمترین جنبه‌هایی که می‌تواند بر روی تعاملات دستگاه‌ها با یکدیگر اثرگذار باشد، میزان آمادگی و قابلیت‌های نرم‌افزاری و برنامه‌های کاربردی این سازمان‌ها برای برقراری تعاملات است. واضح‌است در صورت عدم وجود قابلیت‌های نرم‌افزاری مورد نیاز برای برقراری تعاملات، در صورت مهیا بودن سایر شرایط نیز امکان برقراری تعامل وجود ندارد.
- فرآیند: به تعاملات میان سیستم‌ها و سازمان‌ها از جنبه فرآیندی نیز می‌توان نگریست. همکاری چند فرآیند با یکدیگر از اهداف مورد نظر در این سطح است. یک فرآیند در واقع یک توالی از عملکردها را بر اساس نیازمندی خاصی در سازمان مورد نظر ارائه می‌دهد. معمولا در یک سازمان فرآیندهای متعددی به‌صورت موازی و یا متوالی در حال اجرا هستند. در سازمان‌های شبکه‌ای، فرآیندهای داخلی دو سازمان مختلف به یکدیگر متصل می‌شوند تا یک فرآیند مشترک را ایجاد نمایند. از منظر تعامل‌پذیری فرآیندی، سازمان‌ها می‌بایست به‌شکلی فرآیندها را مدل‌سازی و پیاده‌سازی نمایند که برقراری تعاملات تسهیل گردد.
- کسب‌وکار: در این سطح از تعامل‌پذیری، همکاری به‌صورت هماهنگ در سطح سازمان‌ها/واحدهای سازمانی، علی‌رغم وجود اختلافات موجود در دو کسب‌وکار مختلف (به‌عنوان مثال روش‌های تصمیم‌گیری، مدل‌های کسب‌وکار، قوانین، فرهنگ سازمانی و رویکردهای تجاری و ... مختلف)، مطرح است. هدف از طرح این سطح از تعامل‌پذیری، امکان ایجاد توسعه و به‌اشتراک‌گذاری کسب‌وکار بین سازمان‌ها است.
- امنیت: در این بعد از تعامل‌پذیری، الزامات امنیتی جهت تعاملات بین سازمان‌های مختلف بررسی می‌گردد. در واقع می‌توان گفت این بعد به‌صورت مشترک در میان تمام ابعاد (یعنی امنیت کسب‌وکار، امنیت فرآیند، امنیت برنامه کاربردی و ...) جهت برقراری تعاملات بین سازمانی مطرح است.

شاخص‌های مدل بلوغ تعامل‌پذیری کشور جهت تسهیل کار ارزیابی ارائه شده‌اند. این شاخص‌ها از شکست و تجزیهٔ ابعاد مدل به دست آمده تا همانطور که اشاره شد، ارزیابی کمّی توسط مدل میسر گردد. در جدول ۱ شاخص‌های مربوط به هر بعد و سطح قابل مشاهده است.

۳-۲- روش ارزیابی سطح بلوغ در مدل بلوغ تعامل‌پذیری کشور

یکی از مؤلفه‌های اصلی شکل دهنده مدل بلوغ تعامل‌پذیری کشور، فرآیند ارزیابی بلوغ است. برای ارزیابی می‌توان بلوغ تعامل‌پذیری را از سه منظر مختلف مورد بررسی قرار داد که عبارتند از: تراکنش بین دو سیستم اطلاعاتی (در محدوده یک سازمان یا بین دوسازمان)/ سازمان، سیستم اطلاعاتی و سازمان.

۳-۲-۱- ارزیابی بلوغ تعامل‌پذیری در یک تراکنش بین دو سیستم اطلاعاتی/سازمان

ارزیابی بلوغ تعاملات میان سیستم‌های اطلاعاتی/سازمان‌ها به نهادهای تصمیم‌گیر این امکان را می‌دهد که ضمن آگاهی از وضع جاری بلوغ تعاملات، فرصت برنامه‌ریزی برای بهبود سطح بلوغ تعاملات را به‌دست آورند.

نکته مهمی که در این زمینه می‌بایست مد نظر قرار داد اینست که بُعد برنامه کاربردی از اهمیت بالایی در تعیین سطح بلوغ یک تعامل دارد. دلیل این امر اینست که در صورتی که یک تعامل از نظر قابلیت‌های برنامه کاربردی دارای سطح بالایی نباشد، حتی در صورت مهیا بودن شرایط تعامل‌پذیری در سایر ابعاد بلوغ، باز هم نمی‌توان برقراری تعاملی با سطح بالا را متصور بود. همچنین پرواضح است که قابلیت‌های زیرساختی در تعاملات اولویت بالایی دارد و در صورتی که قابلیت‌های تعامل زیرساختی برای سازمان فراهم نباشد، بررسی سایر ابعاد جهت تعامل‌پذیری بیهوده است.

خروجی روش ارزیابی سطح بلوغ ارائه شده در این مطالعه یک عدد اعشاری خواهد بود. قسمت صحیح این عدد اعشاری در گام اول روش و بر اساس دو بعد زیرساخت و برنامه کاربردی تعیین خواهد شد. قسمت اعشار عدد خروجی نیز در گام دوم و با توجه به شاخص‌های موجود در سایر ابعاد مدل بلوغ تعامل‌پذیری کشور قابل محاسبه است. در نتیجه جهت تعیین سطح بلوغ یک تعامل، پیمودن دو گام، ضروری است.

۱- گام اول: بررسی سطح بلوغ تعامل‌پذیری از بُعد زیرساخت و برنامه کاربردی

برای مشخص کردن سطح بلوغ یک تعامل، ابتدا باید آن را از نظر قابلیت‌های برنامه کاربردی مورد بررسی قرار داد. البته لازم به ذکر است که اگر قابلیت‌های زیرساخت برای تعاملات مهیا نباشد (از شبکه‌های کامپیوتری برای انتقال اطلاعات استفاده نشود)، فارغ از این‌که قابلیت‌های برنامه کاربردی در چه سطحی از بلوغ قرار گرفته، تعامل در سطح اول بلوغ (سطح منفرد) قرار خواهد گرفت. در غیر این صورت، سطح بلوغ برنامه کاربردی در تعامل بیانگر سطح بلوغ کل تعامل نیز خواهد بود.

۲- گام دوم: بررسی سطح بلوغ سایر ابعاد تعامل‌پذیری

پس از پیمودن گام اول و مشخص شدن سطح بلوغ با استفاده از ارزیابی ابعاد زیرساخت و همچنین برنامه کاربردی، نوبت به بررسی سایر ابعاد تعامل‌پذیری (داده و اطلاعات، فرآیند، کسب‌وکار و امنیت) می‌رسد. در این گام، قسمت اعشاری عدد خروجی مشخص خواهد

شد. این مقدار بر اساس شاخص‌های مطرح در جدول شاخص‌ها قابل محاسبه است. در مدل بلوغ ارائه شده، برای هر کدام از شاخص‌های موجود، بسته به سطحی که در آن قرار دارند امتیازی در نظر گرفته شده است. بخش اعشار عدد خروجی در این گام، از حاصل‌ضرب امتیازات در نظر گرفته شده برای هر شاخص در سطوح مختلف حاصل می‌شود.

شایان ذکر است برای مواردی که امتیاز دو طرف یک تعامل (دو سیستم اطلاعاتی یا دو سازمان)، با یکدیگر متفاوت است (به‌طور مثال، در حوزه کسب‌وکار یا امنیت)، ناگزیر، امتیاز کمتر ملاک خواهد بود.

جدول ۱: شاخص‌های مطرح در مدل بلوغ تعامل‌پذیری کشور

بعد	سطح	شاخص‌ها		
زیرساخت	سطح اول	رسانه‌های جداشدنی (۳)		کاغذ (۱)
	سطح دوم تا دهم	شبکه ملی اطلاعات (۵)	شبکه اختصاصی (۳)	اینترنت (۱)
		انطباق بیش از ۹۰٪ استانداردهای سازمان با فهرست استاندارد فنی (۷) انطباق بین ۶۰٪ تا ۹۰٪ استانداردهای سازمان با فهرست استاندارد فنی (۵) انطباق بین ۳۰٪ تا ۶۰٪ استانداردهای سازمان با فهرست استاندارد فنی (۳) انطباق کمتر از ۳۰٪ استانداردهای سازمان با فهرست استاندارد فنی (۱)		
داده و اطلاعات	تمامی سطوح	شمای ملی (۷) شمای استاندارد، مرجع یا حداقل به‌روش (۵)		شمای توافقی چندجانبه (۳) شمای توافقی دوجانبه (۱)
		زمینه داده با استفاده از روش‌های کاملا رسمی (مثلا با استفاده از هستان‌شناسی) تعیین شده است (۷) زمینه داده با استفاده از روش‌های نیمه رسمی تعیین شده است۱ (۵) زمینه داده با استفاده از روش‌های غیر رسمی تعیین شده است (۳) زمینه داده تعیین نشده است (۱)		
		جریان داده در چرخه بهبود قرار گرفته است (۷) جریان داده پایش می‌شود (۵)		جریان داده مدل شده است (۳) جریان داده مدل نشده است (۱)
برنامه کاربردی	سطح اول	ورود اطلاعات با دیسک (۳)		ورود دستی اطلاعات (۱)
	سطح دوم	یکپارچه‌سازی برنامه‌های کاربردی سازمانی یا EAI/ یکنواختی و هماهنگی جریان اطلاعات (۵) مرور وب یا Web Browsing (۳)		انتقال فایل‌های اطلاعاتی یا DFT (۱)
		رویکرد شی‌گرایی به جای ساخت‌یافته (۱)		
		معماری لایه‌ای به جای معماری یکپارچه (۱)		
	سطح سوم	وجود مولفه‌ها۲ با دانه‌بندی مناسب و قابلیت استفاده مجدد بالا (۵) وجود مولفه‌ها با دانه‌بندی و قابلیت استفاده مجدد متوسط (۳) وجود مولفه‌ها با دانه‌بندی نامناسب و قابلیت استفاده مجدد پایین (۱)		
	سطح چهارم	شناسایی/تعریف برخی سرویس‌ها (۱)		
	سطح پنجم	بین ۷۵٪ تا ۹۰٪ از عملکردهای کسب‌وکاری سازمان به صورت سرویس درآمده و منتشر شده (۷) بین۵۰٪ تا ۷۵٪ از عملکردهای کسب‌وکاری سازمان به صورت سرویس درآمده و منتشر شده (۵) بین ۲۵٪ تا نیمی از عملکردهای کسب‌وکاری سازمان به صورت سرویس درآمده و منتشر شده (۳) کمتر از ۲۵٪ از عملکردهای کسب‌وکاری سازمان به صورت سرویس درآمده و منتشر شده (۱)		
	سطح ششم	یکپارچگی معماری سرویس‌گرا با فرآیند توسعه در سراسر سازمان (۱)		
		بالای ۹۰٪ از عملکردهای کسب‌وکاری سازمان به صورت سرویس درآمده و منتشر شده (۱)		
	سطح هفتم	وجود برنامه‌های کاربردی کاملا یکپارچه و قابل دسترس از طریق سازوکار SSO (۱)		
	سطح هشتم	وجود سرویس‌های مرکب (۱)		
	سطح نهم	GSB (۳)		ESB (۱)
	سطح دهم	معماری پویا بر اساس سرویس‌های مرکب (۱)		

فرآیند	سطح اول	فرآیندهای یکپارچه و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده یا مهندسی مجدد شده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح دوم	فرآیندهای یکپارچه (بر اساس EAI) و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده (بر اساس EAI) یا مهندسی مجددشده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح سوم	فرآیندهای یکپارچه (بر اساس مولفه‌ها) و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده (بر اساس مولفه‌ها) یا مهندسی مجدد شده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح چهارم	فرآیندهای یکپارچه (بر اساس سرویس‌ها) و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده (بر اساس سرویس‌ها) یا مهندسی مجدد شده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح پنجم	فرآیندهای یکپارچه (بر اساس سرویس‌ها) و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده (بر اساس سرویس‌ها) یا مهندسی مجدد شده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح ششم	فرآیندهای یکپارچه (بر اساس سرویس‌ها) و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده (بر اساس سرویس‌ها) یا مهندسی مجدد شده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح هفتم	فرآیندهای یکپارچه (بر اساس پنجره واحد ارائه خدمات) و مهندسی مجدد شده (۷) فرآیندهای یکپارچه‌شده (بر اساس پنجره واحد ارائه خدمات) یا مهندسی مجدد شده (۵)	فرآیندهای مدل شده (۳) فرآیندهای شناسایی شده (۱)
	سطح هشتم	تحلیل و پایش فرآیندهای کسب‌وکار در زمان اجرا (۵) گسترش فرآیندهای کسب‌وکار به سازمان‌های خارجی از طریق یکپارچگی سرویس‌ها (۳) پشتیبانی فرآیندهای کسب‌وکار از طریق همنواسازی سرویس‌ها/ ارتباط کامل میان فرآیندهای کسب‌وکار و سرویس‌ها (۱)	
	سطح نهم	بازمهندسی فرآیندهای کسب‌وکار (توسعه یافته از طریق سرویس‌های مجازی) در زمان اجرا (۵) تحلیل و پایش فرآیندهای کسب‌وکار (توسعه یافته از طریق سرویس‌های مجازی) در زمان اجرا (۳) پشتیبانی فرآیندهای کسب‌وکار از طریق سرویس‌های مجازی (۱)	
	سطح دهم	پشتیبانی از فرآیندهای کسب‌وکار قابل پیکربندی در زمان اجرا (خودسازمانده) از طریق استفاده از سرویس‌های پویا (۱)	
کسب‌وکار	تمامی سطوح	توافق کامل در تعاملات (۷) توافق زیاد در تعاملات (۵)	توافق کم در تعاملات (۳) بدون توافقنامه در تعاملات/یکپارچگی موقت و خاص منظوره (۱)
		هم دانش صریح و هم سیستم مدیریت دانش در سازمان وجود دارد (۷) دانش سازمانی صریح در سازمان وجود دارد، اما مدیریت نشده است (۵) نیاز به دانش سازمانی مطرح است و دانش ضمنی در سازمان وجود دارد (۳) هیچگونه دغدغه و یا تعریفی از مدیریت دانش در سازمان مطرح نیست (۱)	
		تغییر فرهنگ سازمانی جهت حرکت به سمت یکپارچگی (۷) وجود آموزش‌ها و مشوق‌های لازم جهت حرکت به سمت یکپارچگی (۵)	اراده مدیریتی برای حرکت به سمت یکپارچگی (۳) بدون تصمیم برای حرکت به سمت یکپارچگی (۱)
		چشم انداز، راهبردها و سیاست‌های مربوط به تعامل‌پذیری در چرخه اجرا، پایش و بهبود قرار گرفته است (۷) چشم انداز، راهبردها و سیاست‌های مربوط به تعامل‌پذیری، در لایه‌های فرآیند، برنامه‌کاربردی، داده، زیرساخت و امنیت اجرایی شده است (۵) چشم انداز، راهبردها و سیاست‌های مربوط به تعامل‌پذیری مشخص شده است (۳). چشم انداز، راهبردها و سیاست‌های مربوط به تعامل‌پذیری مشخص نشده است (۱)	
		مسئولیت‌ها و نقش‌ها در حوزه تعامل‌پذیری در چرخه اجرا، نظارت و بهبود قرار گرفته است. (۷) مسئولیت‌ها و نقش‌ها در حوزه تعامل‌پذیری اجرا شده است. (۵) مسئولیت‌ها و نقش‌ها در حوزه تعامل‌پذیری مشخص شده است. (۳) مسئولیت‌ها و نقش‌ها در حوزه تعامل‌پذیری مشخص نشده است. (۱)	
		بودجه مربوط به تعامل‌پذیری در چرخه تخصیص، نظارت و بهبود قرار گرفته است. (۷) بودجه مربوط به تعامل‌پذیری تخصیص یافته است. (۵)	بودجه مربوط به تعامل‌پذیری تعیین شده است. (۳) بودجه مربوط به تعامل‌پذیری تعیین نشده است. (۱)
امنیت	تمامی سطوح	امنیت بالا در حوزه زیرساخت (۷)۳ امنیت متوسط در حوزه زیرساخت (۵)	امنیت ضعیف در حوزه زیرساخت (۳) عدم رعایت موارد امنیتی در حوزه زیرساخت (۱)
		امنیت بالا در حوزه داده (۷) امنیت متوسط در حوزه داده (۵)	امنیت ضعیف در حوزه داده (۳) عدم رعایت موارد امنیتی در حوزه داده (۱)
		امنیت بالا در حوزه نرم‌افزار (۷) امنیت متوسط در حوزه نرم‌افزار (۵)	امنیت ضعیف در حوزه نرم‌افزار (۳) عدم رعایت موارد امنیتی در حوزه نرم‌افزار (۱)

نکتــه دیگر این‌کــه، اگر هــدف ارزیابی میــزان تعامل‌پذیری بین دو ســازمان باشد و تعاملات دو ســازمان محدود به یک تراکنش نباشد، اگر سطح بلوغ همه تراکنش‌های تعاملی یکسان باشد، میانگین امتیاز تراکنش‌های مختلف منظور می‌شــود. در غیراین‌صورت، باید ســطح بلوغ به ازای هر تراکنش به‌صورت جداگانه اظهار شود.

۳-۲-۲- ارزیابی بلوغ تعامل‌پذیری در یک سیستم اطلاعاتی

جنبــه دیگری که می‌تواند در ارزیابی بلــوغ تعامل‌پذیری مورد توجه قرار گیرد، بررســی وضع جاری تعامل‌پذیری در ســطح سیستم‌های اطلاعاتی می‌باشــد. ارزیابی بلوغ تعامل‌پذیری سیستم‌ها به سازمان‌ها و همچنین نهادهای مرتبط این امکان را می‌دهد تا شــناختی کلی از قابلیت و آمادگی سیســتم‌ها برای برقراری تعامل با ســایر سیستم‌ها کســب کنند که می‌تواند عاملی مهم در برنامه‌ریزی برای بهبود بلوغ تعامل‌پذیری باشد.

برای اندازه‌گیری سطح بلوغ تعامل‌پذیری یک سیستم اطلاعاتی، مشابه بخش قبل عمل خواهد شــد. تنها تفاوت این اســت که امتیاز شاخص میزان توافق در تعاملات (در بُعد کسب‌وکار) لحاظ نخواهد شد.

۳-۲-۳- مقایسه بلوغ تعامل‌پذیری در سازمان‌ها

جنبــه دیگری که می‌تواند در ارزیابی بلــوغ تعامل‌پذیری مورد توجه قــرار گیرد، تعامل‌پذیری در ســطح ســازمان می‌باشــد. ارزیابی بلوغ تعامل‌پذیری ســازمان‌ها به سازمان‌ها و همچنین نهادهای مرتبط این امکان را می‌دهد تا شــناختی کلی از قابلیت و آمادگی ســازمان برای برقراری تعامل با سایر سازمان‌ها کسب کنند که می‌تواند عاملی مهم در برنامه‌ریزی برای بهبود بلوغ تعامل‌پذیری باشد.

برای ارزیابی بلوغ تعامل‌پذیری در یک سازمان، ابتدا بلوغ تعامل‌پذیری سیستم‌های اطلاعاتی مورد اســتفاده در آن سازمان، که در تعاملات نقــش دارنــد، مورد بررســی قــرار می‌گیرد. اگر ســطح بلــوغ همه سیستم‌های اطلاعاتی یکسان باشد، میانگین وزنی امتیاز سیستم‌های مختلف منظور می‌شــود. ضریب هر سیســتم اطلاعاتی در محاســبه میانگین وزنی، درصد پوشش فرایندهای کسب‌وکاری سازمان توسط آن سیستم اطلاعاتی است. در محاسبه این ضریب، صرفا فرایندهایی درنظر گرفته می‌شــوند که محدود به یک سیستم اطلاعاتی نیستند و اجرای آن‌ها به تعامل حداقل دو سیســتم نیاز دارد. اگر فرایندهایی با مشــخصات فوق وجود داشته باشند که توسط هیچ سیستمی پوشش داده نشــوند، در تعیین وزن هیچ‌یک از سیستم‌ها مشارکت نداشته و در نتیجه، به کاهش میانگین امتیاز ســازمان منجر خواهند شــد. اگر سطح بلوغ همه سیستم‌های اطلاعاتی یکسان نباشد، باید سطح بلوغ به ازای هر سیســتم به همراه وزن آن سیســتم در کسب‌وکار سازمان به‌صورت جداگانه اظهار شود.

۴-نتیجه‌گیری

با توجه به این‌که معماری ســرویس‌گرا یکــی از فناوری‌های اخیر جا افتاده در سازمان‌هاســت، مدل بلوغ تعامل‌پذیری کشــور نیز با تاکید بر مفهوم معماری ســرویس‌گرا توسعه داده شــد. این مدل شامل ده ســطح بلوغ و شش بعد اســت. در هریک از ابعاد، شاخص‌هایی برای ارزیابی ســطح بلوغ سازمان/سیستم اطلاعاتی معرفی شده است که با تعیین شاخص‌های مناسب یک ســازمان/ سیستم اطلاعاتی از جنبه زیرســاخت و برنامه کاربردی، و سپس بررسی سایر ابعاد، سطح بلوغ آن سیســتم/ سازمان به‌دست می‌آید. در این مدل بلوغ، تعامل‌پذیری از ســه جنبهٔ مختلف تراکنش بین دو سیستم اطلاعاتی/سازمان، یک سیستم و داخل سازمان مورد بررسی قرار گرفته است.

موارد زیر را می‌توان به‌عنوان جهت‌گیری‌های آتی برای کارهای بیشتر در این زمینه مدنظر قرار داد:

- ایجــاد ابزاری برای ارزیابی بلوغ تعامل‌پذیری ســازمان‌ها بر مبنای مدل بلوغ ارائه شده
- بــه کارگیری مدل بلوغ ارائه شــده بــر روی چند ســازمان ایرانی به‌عنوان مورد مطالعه
- افزودن شاخص‌های بیشتر به هریک از سطوح و ابعاد

مراجع

1- Roland Jochem, ENTERPRISE INTEROPERABILITY ASSESSMENT, 8th International Conference of Modeling and Simulation - MOSIM'10 - May 10-12, 2010 - Hammamet - Tunisia

2-Mark Knight, Pacific Northwest National Laboratory Interoperability Project, Partners Meeting, AEP Gahanna, May 10, 2017," Interoperability Maturity Model".

3-Andras R. Szakal, "Open Group Service Integration Maturity Model (OSIMM)", Open Group, 2009.

4-Meier, F. (2006). Service Oriented Architecture Maturity Models-A guide to SOA adoption. Institutionen för kommunikation och information.

5-Levels of Information Systems Interoperability (LISI), C4ISR Architectures Working Group, 1998.

6-Cristina Campos, Ricardo Chalmeta , Reyes Grangel & Raúl Poler (2013) Maturity Model for Interoperability Potential Measurement, Information Systems Management, 30:3, 218-234,

7-Clark, Thea, and Richard Jones. «Organizational interoperability maturity model for C2.» In Proceedings of the 1999 Command and Control Research and Technology Symposium, pp. 1-13. 1999.

8-Athena Consortium. (2004). Enterprise interoperability maturity model (EIMM). In ATHENA IP (Advanced Technologies for interoperability of Heterogeneous Enterprise Networks and their Applications Integrated Project).

9-Van Staden, S., and N. Mbale. «The Information Systems Interoperability Maturity Model (ISIMM): towards standardizing technical interoperability and assessment within government.» International Journal of Information Engineering and Electronic Business 4, no. 5 (2012): 36.

۱۰- ح. حاجی حسینی و همکاران، «تعیین شاخصهای اندازه‌گیری و مدل بلوغ قابلیت تعامل‌پذیری فنی»، پژوهشــکده سیاســتگذاری و مدیریت راهبری فاوا، تیرماه ۱۳۹۵.

پی‌آیند روایات آموزشی

روایت یکم: تجربیاتی در تدوین و ارائهٔ گفتمانی برنامه درسی با بومی‌سازی بهترین تجارب موجود در درس مدیریت و برنامه‌ریزی راهبردی فناوری اطلاعات

سید ابراهیم ابطحی
استادیار دانشکده مهندسی کامپیوتر- دانشگاه صنعتی شریف
نایب رئیس انجمن انفورماتیک ایران
پست الکترونیکی: abtahi@sharif.edu

مقدمه

در پاسخ به ابتکار و فراخوان مشترک کرسی یونسکو در آموزش مهندسی و انجمن آموزش مهندسی ایران در زمستان سال گذشته، در موضوع اشتراک تجربیات یاددهی- یادگیری در آموزش مهندسی، اقدام به ارسال چهار نمونه از تجارب تدریسی خود به این فراخوان نمودم. در پایان ماه گذشته داوران این فراخوان، هفت تجربه ارسالی از جمله دو مورد مربوط به نگارنده را، در صورت هفت منتخب این تجارب، اعلام نمودند. این اقدام شایسته با اقدامات ترویجی می‌تواند ثمرات اثربخشی در گردآوری یک حافظه زمانمند برای تدوین و انتقال تجارب آموزشی و ترویج گونه‌های موفق و ارزشمند آن برای اجرا و ارتقاء بین استادان جوان را به‌دنبال داشته باشد. به همین اعتبار بر آن شدیم از این شماره صفحاتی را به درج این گونه تجارب با عنوان پی‌آیند (سریال) روایات آموزشی، اختصاص دهیم. از تمامی همکاران دانشگاهی مجرب و جوان دعوت می‌کنیم با ارسال تجارب نوآورانه آموزشی خود به غنای این صفحات و تعمیق این اقدام فرهنگی یاری رسانند. ما آماده نشر این تجارب ارزنده و معرفی فرهیختگان نوآور مبدع آن به جامعه انفورماتیک کشور هستیم. روایت دوم تا پنجم برای دروس آداب فناوری اطلاعات، مهندسی نرم افزار، شیوه‌های ارائه مطالب علمی و فنی و مدیریت پروژه‌های فناوری اطلاعات را در شماره‌های بعد انتشار خواهیم داد و امیدواریم با همت دوستان عزیز مدت‌ها انتشار این صفحه با دروس مختلف استمرار یابد.

روایت یکم

برنامه درسی درس مدیریت و برنامه‌ریزی راهبردی فناوری اطلاعات[1] را نگارنده در اوائل دهه هشتاد در اولین ویرایش برنامه درسی اعلام شده توسط وزارت علوم، تحقیقات و فناوری، تهیه و طی ۱۲ سال در ۱۴ ترم از سال ۱۳۸۵ تا ۱۳۹۷، یک ترم در میان آن را در دانشده مهندسی کامپیوتر دانشگاه صنعتی شریف، عرضه و در چندین گونه متفاوت، به اجرا گذارد. به اعتقاد نگارنده در برنامه‌های درسی رشته‌های مهندسی رایانه و فناوری اطلاعات برخی دروس که با جنبه‌های مهارتی، به تغییر یا ارتقاء دیدگاه یا منظر دانشجویان نیاز دارند، مناسب است با ماهیت گفتمانی[2] عرضه شوند. گفتمانی مبتنی بر گفتگو[3] سه جانبهٔ مدرس، دانشجو و محتوای درس.

1-ITSMP : Information Technology Strategic Management and Planning : مبرفا
مدیریت و برنامه ریزی راهبردی فناوری اطلاعات
2- Discourse Based
3- Dialogue

بـا تکیـه بر کتاب درسـی می‌تواند در رونـدی بالغ شـونده و تعالی بخـش، این ارتقای منظر شـکل بگیرد. به‌عنـوان نمونه درس تحلیل و طراحی سـامانه‌های اطلاعاتی رایانه‌ای، در ایـن مجموعه از طریق پروژه درسـی باید بتواند، نگاه برنامه‌ای دانشـجو،که پس از گذراندن دروس برنامه‌نویسـی حاصل شـده است را به نگاه سـامانه‌ای، ارتقاء دهد. به همین سـیاق درس مدیریت و برنامه‌ریزی راهبردی فناوری اطلاعات پس از درس پیش‌نیاز خود، یعنی مدیریت پروژه‌های فناوری اطلاعـات[۴]، باید بتواند نگاه پروژه‌ای حاصله را به نگاه سـازمانی ارتقاء دهـد که ماهیت تحـول کیفی دارد. زیرا نگاه جزئی‌نگر سـامانه‌ای و پروژه‌ای در ارتقاء به نگاه سـازمانی، باید از جزئی‌نگری رها شـده و با نگاه اجمالی مبتنی بر شـناخت و خبرگـی، پس از کفایت و نه اتمام تحلیل همه جانبه، راه‌حلی را برای وضعیت مطلوب معماری سازمانی با توجه به بهترین تجارب موجود طراحی و برای اجرا در برنامه گذار، پس از فاصله سنجی، تبدیل به سبدهایی از طرح‌های عملیاتی نماید. در ارائه گفتمانی دروس، زنجیره تعالی بخش مولفه‌های درسی، نقشی کلیدی دارند و چیدمان مناسب بدنه‌های دانشی[۵] مرتبط در این میان، نقشی اصلی ایفا می‌کنند.

مشـکل بعدی مثال‌ها و بهترین تجارب[۶] موجود مندرج در کتاب‌های درسی مرتبط با این درس بود که تناسب آن با وضعیت ما و شناخت از ماهیت آن‌ها، برای دانشـجویان دشوار بود. نگارنده تجارب ده ساله خـود در محیط‌های واقعی در کشـور در این حـوزه را با اخذ مجوز آموزشـی از کارفرمایـان، جایگزین مثال‌های کتاب‌هـا نمود تا برای دانشـجویان ملموس بوده و انجام ایـن پروژه‌های بزرگ را باور کنند. دشـواری پایانی، انتخاب کتاب درسـی دانشـجویان و ابزار رایانه‌ای مناسب برای انجام مطالعات راهبردی فناوری اطلاعات بود. با بررسی آنچه در دنیا انجام شـده بود سـرانجام کتاب خانم هانشکه[۷] با عنوان مدیریت راهبـردی فناوری اطلاعات[۸] انتخـاب گردید. تجارب عملی ایشان در شرکتی در مونیخ با ابداع ابزاری رایانه‌ای برای مستندسازی به نام ایتراپلان[۹] و الگوی مستندسازی کمینه‌گرا[۱۰]ی شمایلی[۱۱] مشابه مـدل معماری سـازمانی تک برگ آدریـن گریگور[۱۲]، بـه این کتاب به‌عنوان یکی از کتب درسـی اصلی وجاهت خاص می‌بخشید. کتاب خانم هانشـکه ویژگی خاص و جالـب دیگری هم دارد آن هم توصیه روشـی برای تحلیل و طراحی سـازمان و لایه‌های آن، به‌عنوان نگاه منظـره گرا[۱۳] با منطق رویت از فاصله مناسـب، نـه چندان دور و نه چندان نزدیک با فاصله‌ای از سـازمان که نه در جزئیات غرق شوید و نه آن میزان کلان‌نگری که در آن خاصه‌های سـازمان مورد معماری فراموش شود. این بن انگارهٔ[۱۴] خانم هانشکه برای الگوی گفتمانی ارائه این درس، کلیدی اصلی و راهگشـا شـد. دشـواری نهائی حجم زیاد مطالـب موجود و قابل ارائه و لازم، بـرای عرضه این درس بود که به گزینی آن و سلسه مراتب متکامل مفاهیم، قاعده‌ای بود که در تدوین جزئیات برنامه درسی، لحاظ گردید.

انتخاب این سـاختار متکامل به گونه‌ای که به‌تدریج دانشجو را آماده مواجهه با دشواری های فهم مطالب کتاب درسی با یادگیری متکامل بنمایـد اقدام بعدی بود. به همین دلیـل گام یا چرخهٔ آغازین درس، واژه شناسی حوزه مدیریت و برنامه‌ریزی راهبردی به اضافه مروری بر تعاریف و مفاهیم پایه فناوری اطلاعات انتخاب شد.

در گام یـا چرخهٔ دوم یک مدل سـنتی و مهارتی به شـکل ترکیبی، برای انجام برنامه‌ریزی راهبردی با مثال و تمرین برای آموزش انتخاب شد. مدلی مرکب از شـش مدل: تحلیل محیط عمومی کسب‌وکار[۱۵]، ارزیابـی عوامل داخلی[۱۶](برای اسـتخراج نقاط قوت و ضعف)، ارزیابی عوامل خارجی[۱۷] (برای استخراج فرصت‌ها و تهدیدها)، چارچوبی برای تلفیـق داده‌ها و خلق راهبردهای کسـب‌وکار با تعیین مناسـب‌ترین گونه راهبردها[۱۸] (تهاجمی، محافظه کارانه، تدافعی یا رقابتی)، تحلیل سوات[۱۹] (نگاشت فرصت‌ها، تهدیدها، نقاط قوت وضعف) برای استخراج راهبردها و در نهایت مدل ماتریس کمّی برنامه‌ریزی راهبردی[۲۰] برای اولویت‌بندی راهبردها، برای تصمیم‌گیری نهائی و انتخاب راهبردها.

گام یـا چرخهٔ سـوم به معرفی تدوین مدل- پایـه برنامه راهبردی با مدل‌هـای نامدار مختص انواع سـازمان اختصاص داشـت. مثل مدل برایسـون[۲۱]، مخصوص سازمان‌های ویژه سالار[۲۲] نظیر پژوهشکده‌ها یا دانشگاه‌ها.

در گام یـا چرخـهٔ چهارم معرفی و بیـان مدل فرآینـدی انواعی از مطالعات راهبردی صـورت می‌گرفت. انواعـی از مطالعاتی راهبردی در یک توالی تکاملی شـامل: برنامه‌ریزی راهبردی کسب‌وکار سازمان (برک)[۲۳]، برنامه‌ریزی راهبردی سامانه‌های اطلاعاتی سازمان (برسا)[۲۴]، مدیریت منابع اطلاعاتی سـازمان (مماس)[۲۵]، مدیریت منابع دانشـی سـازمان[۲۶]، برنامه راهبردی فناوری اطلاعات سازمان (برفا)[۲۷]، برنامه جامع راهبـردی فناوری اطلاعـات سـازمان[۲۸]، برنامه‌ریزی معماری

4- Information Technology Project Management
5- BOK : Body Of Knowledge
6- Best practices
7- Inge Hanschke
8- Inge Hanschke , Strategic IT Management, Springer,2016.
9- Iteraplan
10- Minimalism
11- Iconic
12- Adrian Grigoriu's One-Page Architecture
13- Landscape View

14-Paradigm
15- PEST : Political, Economic, Social, Technological
16- IFE : Internal Factor Evaluation
17- EFE : External Factor Evaluation
۱۸- SPACE : (ES) و قدرت مالی (FS) و ثبات محیطی(IS) و قدرت صنعت (CA) برآیند مزیت رقابتی
19- SWOT : Strengths , Weaknesses , Opportunities , Threats
20- QSPM : Quantitative Strategic Planning Matrix
21- Braison
22- Ad-HOCracy
23- BSP : Business Strategic Planning
24- ISP : Information systems Strategic Planning
25- IRM : Information Resources Management
26- KRM : Knowledge Resources Management
27- ITSP : Information Technology Strategic Plan
28- ITSMP : Information Technology Strategic Master Plan

برنامه زمان‌بندی جلسات دروس		ترم دوم : 98-97		زمان جلسات: یکشنبه‌ها و سه شنبه‌ها 13:30 الی 15	
عنوان درس مدیریت و برنامه ریزی راهبردی فناوری اطلاعات	تعداد واحد: 3	شماره درس: 40448	پیش‌نیاز : مدیریت پروژه های فناوری اطلاعات	مدرس: سیدابراهیم ابطحی	تعداد دانشجو: 16 نفر

هفته	زمان	موضوع جلسه	شماره جلسه	زمان	موضوع جلسه	شماره جلسه
1	97/11/13	معرفی درس و برنامه درسی	1	97/11/15	واژه شناسی مدیریت و برنامه ریزی راهبردی	2
2	97/11/20	شهادت حضرت فاطمه (س) - تعطیل	3	97/11/22	سالروز پیروزی انقلاب اسلامی - تعطیل	4
3	97/11/27	نمای 360 درجه ی برنامه ریزی راهبردی سنتی- 1	5	97/11/29	نمای 360 درجه ی برنامه ریزی راهبردی سنتی- 2	6
4	97/12/4	نمای 360 درجه ی برنامه ریزی راهبردی سنتی- 3	7	97/12/6	مای 360 درجه ی برنامه ریزی راهبردی سنتی- 4	8
5	97/12/11	IFE + EFE +SPACE + SWOT + QSPM	9	97/12/13	تدوین مدل – پایه برنامه راهبردی سازمان -1	10
6	97/12/18	تدوین مدل – پایه برنامه راهبردی سازمان -2	11	97/12/20	انواع مطالعات راهبردی سازمان از کسب و کار تا فناوری -1	12
7	97/12/25	انواع مطالعات راهبردی سازمان از کسب و کار تا فناوری -2	13	97/ 12/27	معماری اطلاعات سازمان برای مدیران -1	14
8	98/1/17	معماری اطلاعات سازمان برای مدیران -2	15	98/1/19	آزمون میان ترم	16
9	98/1/24	معماری اطلاعات سازمان برای مدیران -3	17	98/1/26	برفای هانشکه (ف 1)	18
10	98/1/31	برفای هانشکه (ف 2)	19	98/2/2	معماری سازمان هانشکه (ف 3) – 1	20
11	98/2/7	معماری سازمان هانشکه (ف 3) – 2	21	98/2/9	مدیریت منظره فای هانشکه (فصل 4)- 1	22
12	98/2/14	مدیریت منظره فای هانشکه (فصل 4)- 2	23	98/2/16	استانداردهای فنی معماری سازمان هانشکه (ف 5)	24
13	98/2/21	استانداردهای فنی معماری سازمان هانشکه (ف 6)	25	98/2/23	مدلهای مرجع ، سیاست نامه ، بیانیه تغییر و (NEAF)	26
14	98/2/28	مروری بر روشگان های معماری سازمان	27	98/2/30	برفا از نگاه کونیگزبرگ	28
15	98/3/4	مدلهای بلوغ معماری سازمانی	29	98/3/6	معماری سازمانی در عصر تحول رقمی	30

زمان آزمون‌میان‌ترم: 98/1/19	زمان آزمون پایان ترم 98/3/25	زمان ارائه امتحانک های درسی در جلسات درسی طی ترم	کتاب درسی : برنامه ریزی راهبردی فا هانشکه	دانشگاه صنعتی شریف دانشکده مهندسی کامپیوتر

الگوی ارزیابی تجمیعی و تکوینی دروس	دانشگاه صنعتی شریف دانشکده مهندسی کامپیوتر	ترم دوم : 98-97

عنوان درس: مدیریت و برنامه ریزی راهبردی فناوری اطلاعات	تعداد واحد: 3	شماره درس: 40448	پیش نیاز:مدیریت پروژه های فناوری اطلاعات	مدرس: سید ابراهیم ابطحی	تعداد دانشجو: 16 نفر

ردیف	شکل ارزیابی	الگوی ارزیابی	امتیاز ارزیابی	زمینه و موضوع کار یا ارزیابی	شکل اجرا	گونه ارزیابی	زمان تحویل و ارزیابی
1	آزمون میان ترم	تجمیعی	6 نمره	مطالب کلاسی و وبگاه درسی	انفرادی	کتاب بسته	98/1/19
2	آزمون پایان ترم	تجمیعی	8 نمره	تمام کتاب درسی + مطالب کلاسی و وبگاه درسی	انفرادی	کتاب بسته	98/ 3/25
3	سه امتحانک	تدریجی و تکوینی	6 نمره	موضوع امتحانک ها : مفاهیم و الگوهای برنامه ریزی راهبردی سنتی ، مدل های نامدار برنامه ریزی راهبردی ، معماری سازمانی	انفرادی	حل مسئله و شناخت مفاهیم	امتحانک ها پس از پایان تدریس مفاهیم مندرج در آن گرفته خواهد شد
4	مطالعه انفرادی داوطلبانه مصوب	تکوینی	2+ نمره	از بین داوطلبان مصوب هر موضوع تنها یکنفر با بیشترین امتیاز این دو نمره اضافی را میتواند بگیرد ARCHIMATE , BMM , ITERAPLAN	انفرادی	ارائه نمایشی	تا اول خرداد 97

موضوعات موارد ارزیابی تکوینی درس

1 تمرینک ها و امتحانک های درسی	در حوزه های : تعاریف و مفاهیم و برنامه ریزی راهبردی سنتی ، برنامه ریزی راهبردی مدل- پایه نامدار و معماری سازمانی
2 مطالعه انفرادی داوطلبانه مصوب	ARCHIMATE , BMM , ITERAPLAN
بهترین تجارب موجود ایران	برنامه جامع راهبردی قاوای سازمان میراث فرهنگی ، معماری اطلاعات آموزش پرورش ، برنامه ریزی راهبردی فناوری اطلاعات تاک و شتات

سازمان (برمس)[29] و برنامه‌ریزی معماری اطلاعات سازمان[30].
در گام یـا چرخه پنجـم تفصیلی از معماری سـازمانی برای مدیران کـه یک اجرای کارگاهی داشـت که در آن بـر دو مبحث مهم یعنی چارچوب زکمن[31] و مدل‌های همترازی راهبردی[32] نظیر هندرسـون – ونکاترامن[33] و لوفتمن[34] تاکید می‌شـد و روش و نتایج یک مطالعه

29- EAP : Enterprise Architecture Planning
30- EIAP : Enterprise Information Architecture Planning
31- Zachman, Enterprise Architecture Framework
32- Strategic Alignment Models
33- Henderson - Venkatraman
34- Lofftman

معماری سازمانی در سازمانی بزرگ در ایران، همراه با آن مرور می‌گردید.

در گام یا چرخه ششم کتاب درسی هانشکه که پیش نیازهای یادگیریش در پنج گام پیشین فراهم شده بود بعد از آزمون میان ترم طی نه جلسه تدریس می‌شد.

چرخه و گام هفتم، بخش آخر درس طی پنج جلسه به بیان تجارب عملی مدرس و تازه‌های مطالعات راهبردی فناوری اطلاعات و معماری سازمانی اختصاص داشت. طی این جلسات ابداعات عملی مدرس در زمینه تدوین سیاست نامه[35] و بیانیه تغییر[36] برای تسهیل تحویل پروژه‌های معماری سازمانی تدریس می‌شد. سپس مدل‌های مرجع[37] که نتیجه بهترین تجارب موجود[38] بود و مدل ملی معماری سازمانی ایران[39] مطرح می‌گردید. سپس مروری بر انواعی از روشگان[40]های معماری سازمانی و مدل معماری تک برگ آدرین مک گریگور برای حل مشکل مستندسازی معماری سازمانی، مدل ویژه کونیکزبرگ[41] برای برنامه‌ریزی راهبردی فناوری اطلاعات، در انتها مدل‌های بلوغ معماری سازمانی[42] با مروری بر معماری سازمانی در زمانه تحول رقمی[43] پایان می‌یافت.

در پایان نمونه‌ای از برنامه درسی و زمان بندی اجرای این درس به پیوست ارائه می‌گردد.

35- Policy Document
36- Change Manifest
37- Reference Models

38- Best Practices
39- INEAF : Iran National Enterprise Architecture Framework
40- Methodology
41- Konigzberg
42- EA Maturity Models
43-Digital Transform

یک مدیر بزرگ باشید: پنج روش عملی

سیدعلی آذرکار
شرکت مهندسی پدیدپرداز
کمیسیون استاندارد و تدوین مقررات، سازمان نظام صنفی رایانه‌ای استان تهران
پست الکترونیکی: ali.azarkar@pdpsoft.com

۱- چکیده

قولی است مشهور از باری بوهم* که می‌گوید: «مدیریت ضعیف پروژه نرم‌افزاری بیش از هر عامل دیگری می‌تواند هزینه‌های آن را به سرعت افزایش دهد»؛ اگر این قول درست باشد، باید همان قدر که به روش‌های توسعه نرم‌افزار توجه می‌کنیم، به شیوه‌های مدیریتی آن هم توجه کنیم. در این مقاله نویسنده پنج روش عملی را که به مدیران کمک کرده تا بر کار درست متمرکز شده و محیطی را برای موفقیت خلق کنند، شرح می‌دهد.

۲- مقدمه

روزی با دوستی نهار می‌خوردم که به تازگی فرزندانش را از مدرسه بیرون آورده و به خاطر شغل جدیدش به شهر دیگری نقل مکان کرده بود. از او پرسیدم چه جذابیتی در شغل جدید بود که به خاطر آن شهر را ترک کردی؟ پاسخ داد «رییس جدید من».

کدام مدیران این حد از وفاداری را ایجاد کرده‌اند؟ مدیر جدید، مدیر ضعیفی نبود؛ مدیر ضعیف توهمی از پیشرفت را با ایجاد مشغله‌های غیرضروری ایجاد می‌کند. این مدیران بهره‌وری و اخلاق را بین کارکنان تنزل می‌دهند. مدیر جدید مدیر متوسطی هم نبود؛ کسی که فقط کار را انجام می‌دهد ولی نه همیشه کار صحیح را. این دوست من یک مدیر بزرگ پیدا کرده بود، مدیری که به خاطر او نیمی از کشور را مسافرت کرد.

من مدیران متعددی را در شرکت‌های نرم‌افزاری و واحدهای فناوری اطلاعات ملاقات کرده و با آن‌ها تعامل داشته‌ام. آن‌هایی موفق بوده‌اند که در تحقق اهداف اصلی شرکت مشارکت داشته و به توسعه و پیشرفت افراد کمک کرده‌اند. این مدیران دانش حوزه‌ای کافی را برای پاسخ به سوالات اساسی و درک مخاطره دارند. این نوع مدیران قدرت درک فناوری که تیم آن‌ها با آن کار می‌کند را دارند، حتی اگر مهارت‌های لازم را برای پیاده‌سازی آن نداشته باشند؛ علاوه بر آن، همه آن‌ها از الگوها و روش‌های مشابهی مدیریتی تبعیت می‌کنند.

آنچه در ادامه می‌آید، ممکن است شیوه‌ها و وروش‌هایی نباشد که در دانشکده‌های مدیریت تدریس شده یا در کتاب‌های مدیریت پروژه یا مدیریت پروژه‌های نرم‌افزاری نوشته شده است. این‌ها الگوهای عامی هستند که برآمده از مشاهده رفتار مدیران موفق است.

۳- تصمیم بگیرید چه کاری را انجام دهید و چه کاری را انجام ندهید

مدیران موفق فقط کار را انجام نمی‌دهند، بلکه کار درست را انجام

*Barry Boehm

می‌دهنـد. برای شـرکت‌هایی که کسـب‌وکار نرم‌افـزاری دارند، کار درسـت کاری است که کسـب درآمد می‌کند، مشتری جلب می‌کند و از مشـتریان سـودمند حفظ و مراقبت می‌کند. برای فروشگاه‌های فناوری اطلاعات، کار درسـت، کاری اسـت که کسب‌وکار را توان‌مند ساخته تا به شکلی موثر و کارایی اجرا شود.

از خودتان بپرسـید شـرکت شـما چگونه درآمدزایی دارد و چگونه گروه شما در موفقیت شـرکت مشارکت دارد؟ اگر شرکت شما یک محصول نرم‌افزاری برای فروش تولید کرده باشـد، این رابطه روشن اسـت. گاهی از اوقات، این رابطه خیلی روشـن نیست. اگر شما در یک گروه آزمون باشـید، ممکن اسـت از طریق بیان مخاطرات که امکان تصمیم‌گیری درباره نشـرهای مناسـب را فراهم می‌کند، در موفقیت کسب‌وکار سهیم باشـید. اگر در گروه مستندسازی باشید، مستندسـازی خوب و حرفه‌ای راهنماهای نرم‌افزار، تماس‌ها با گروه پشـتیبانی را کاهش داده و تجربه‌کاربـری محصول را بهبود خواهد داد.

هنگامی که بدانید گروه شما چگونه در موفقیت شرکت مشارکت دارد، می‌توانید ماموریت آن را به شکلی روشن و گویا تعریف کنید. ماموریت گروه توسـعه می‌تواند این‌گونه بیان شود: «پیاده‌سازی ویژگی‌هایی از محصول که نیازهای مشـتری را برآورده کرده و برای شرکت برگشت سـرمایه هم داشته باشـد.» زمانی گروهی را مدیریت می‌کردم که در حال توسـعه نرم‌افزاری در حوزه پورتفولیوی سـرمایه‌گذاری بود. این گـروه ماموریت خود را این طورتعییـن کرده بود: «ارایه ارزش‌گذاری دقیق و به‌روز سرمایه‌های ما.»

همـه ما خیلی بیش از یـک کار برای انجـام دادن داریم؛ وجود یک ماموریت روشن به ما کمک می‌کند تا به شکلی راهبردی کارهای مهم را اولویت‌بندی کرده و آن‌هایی را که لازم نیست انجام بدهیم (دست کم نه برای الان یا نه توسط گروه ما)، شناسایی کنیم.

زمانی با یک مدیر آزمون برای شناسایی و تبیین ماموریتی برای گروه آزمون همکاری داشتم، تا از این طریق، همه کارهایی را که گروه باید انجام مـی‌داد اولویت‌بندی کنیم. او ماموریت گروه را این‌گونه تعریف کرد: «ارزیابی و اطلاع‌رسانی مخاطرات فنی و کسب‌وکاری برنامه‌هایی که آزمون می‌کنیم.» او تمام کارهایی که گروه انجام می‌داد را فهرست کرد، ولی یک فعالیت از بقیه جدا ماند: «پشتیبانی فنی قبل از فروش در سمت مشتری.»

دو سـال قبـل، وقتی یک عضـو تیم فروش مریض بـود، این مدیر با فرسـتادن یک آزمون‌گر به مرکز تماس فروش به این تیم کمک کرد. تماس‌هـای فـروش موفقیت‌آمیز بـود و میز فروش درخواسـت کرد کـه همراهی آزمون‌گران با تیم فروش، به ویژه برای مشـتریان مهم، استمرار داشته باشد.

مدیـر آزمـون پی برد که اگر چه بـا این کار او حسـن نیت خود را نشـان داده، ولی پشـتیبانی فنی قبل از فروش در سـمت مشتریان جزو ماموریت‌های گروه آزمون نبوده و نیست. او ضمن بررسی کاری

جدول ۱: کمّی کردن زمان از دست رفته در حالت چندوظیفگی

تعداد کارها	زمان صرف شده برای هر کار	کل زمان کار
۱	۱۰۰	۱۰۰
۲	۴۰	۸۰
۳	۲۰	۶۰
۴	۱۰	۴۰
۵	۵	۲۵

که تیم فروش (شـامل بازدید از مکان‌ها) انجام می‌داد، مشاهده کرد کـه اعـزام نیروهای آزمون به بخش فروش، گـروه آزمون را از انجام کارهایی کـه به ارزیابی و اطلاع‌رسـانی مخاطرات فنـی برنامه‌های کاربردی تحت آزمون کمک می‌کند، باز می‌دارد. او همچنین دریافت کـه نمی‌تواند این مسـئولیت را هم بلافاصله زمیـن بگذارد؛ چرا که بدون حضور آزمون‌گران، بخش فروش که خون حیاتی شـرکت است با مشـکل و اشتباه مواجهه می‌شد. او طی همکاری مشترکی با مدیر بخش فروش، آموزش‌هایی را تدارک دید تا پشـتیبانی تلفنی محدود به تماس‌ها باشد.

تصمیم‌گیری در این خصوص که چه کاری باید انجام شود و چه کاری نباید انجام شـود، به تمرکز روی انجـام کارهای مهم کمک می‌کند؛ کارهایی که در تحقق اهداف اصلی شـرکت نقش و مشـارکت دارند. تدوین یک ماموریت، فایده دیگری هم دارد: اگر افراد گروه شما با این ماموریت آشنا باشند و بدانند چگونه کاری که انجام می‌دهد در تحقق این ماموریت نقش و سهم دارد، قادر خواهند بود برای کارهای روزمره خود تصمیم‌گیری بهتری داشته باشند.

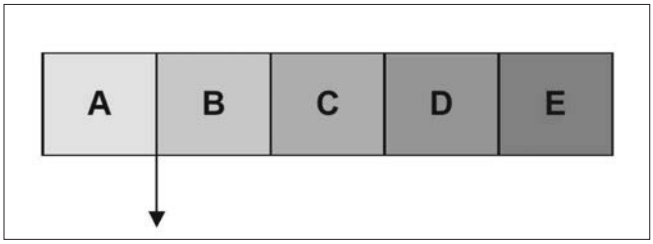
۴- چندوظیفگی[1] را محدود کنید

به نظر می‌رسـد اختصـاص افراد بـه چندین پروژه، ایـن اطمینان خاطـر را به دسـت می‌دهد که همه آن‌ها تمام خواهند شـد. ولی بر خـلاف این باور عمومـی، چندوظیفگی نه تنها سـرعت انجام کار را زیـاد نمی‌کند بلکه باعث کند شـدن انجام آن‌هـا و تاخیر در تحویل هـم می‌شـود. چندوظیفگی بـا ایجاد مشـغله بی‌دلیـل، توهمی از پیشـرفت را ایجاد می‌کند، ضمن آن‌که زمان و اسـتعداد افراد را هم به هدر می‌دهد. آدمیان در جابجایی (سـوییچ کردن) بین موضوعات مختلف، بـه خوبی عمل نمی‌کنند. واینبرگ[2] زمان از دسـت رفته را (به ازای تعداد کارهای موازی) در جدول ۱ به شـکل کمّی بیان کرده است.

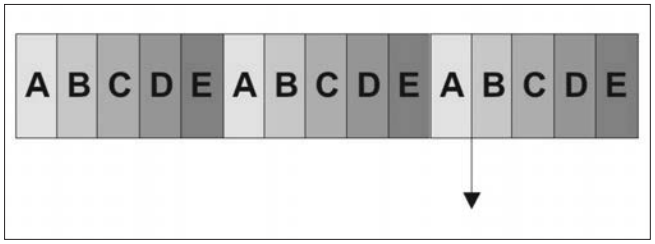
افـراد هنگامی که کار A را کنـار می‌گذارند و به یاد می‌آورند که بایـد به‌کار B بپردازند، زمانی را در این میانه از دسـت می‌دهند.

1- Multitasking

۲- Gerald M. Weinberg (۱۹۳۳-۲۰۱۸، دانشـمند آمریکایی مختص علوم رایانه و روانشناسـی توسـعه نرم‌افزار)



شکل ۱: عملکرد فردی که یک وظیفه در یک زمان به او اختصاص یافته



شکل ۲: عملکرد فردی که پنج وظیفه در یک زمان به او اختصاص یافته

زمانی که لازم است تا یادداشت‌ها و مستندات کار B را به خاطر آورده و یک خط جدید فکری را بازتولید کنند. اختصاص چندین وظیفــه به یک فرد، فقط هنــگام صرفه‌جویی زمانی دارد که فرد فقط دو وظیفه داشــته باشــد که یکی از آن‌ها به طور مشخص و روشــن دارای اولویت بالاتری (نسبت به دیگری) است. فردی که روی یک وظیفه با اولویت بالا کار می‌کند، تا زمانی که مســئول آن اســت یا نمی‌تواند آن را بیشــتر به پیش ببرد، در این فرصت به ســراغ وظیفه بــا اولویت پایین‌تر می‌رود. ایــن می‌تواند اوقات بیکاری فرد را، در مقایســه با حالتی که فقــط یک وظیفه دارد، کاهش دهد.

در حوزه توســعه محصول، می‌توان به این کارها به عنوان «پروژه» یا بخشی از کارهای کاملاً متفاوتی فکر کرد. حضور در دو یا چند پروژه بهره‌وری را نابود می‌کند. تصور کنید ۵ وظیفه همزمان دارید. شــکل ۱ نشان می‌دهد که چگونه تمرکز بر یک وظیفه منجر به تحویل زودتر ارزش می‌شــود. پیکان نشــان می‌دهد که چه زمانــی با اهمیت‌ترین وظیفه (یعنی وظیفه A) پایان می‌یابد.

اگر شــما ۵ وظیفه و فقط یک نفر برای اجرای آن‌ها داشــته باشید، چــه اتفاقی خواهــد افتاد؟ به جای اختصــاص ۵ وظیفه به هر فرد، صفی از وظیفه ها ایجاد کنید. وظیفه هر فرد که تمام شــد، وظیفه بعدی را به او اختصاص دهید. این چندوظیفگی را محدود کرده ولی واقعاً زمان تحویل را بهبود خواهد داد. تصور کنید ۵ وظیفه دارید و همه را به یک نفر محول کرده‌اید؛ با این تاکید که همه این وظیفه‌ها مهم هســتند و باید پیشرفت داشته باشند. فردی که مسئول انجام همــه این وظیفه‌ها اســت، وقت خود را بین این ۵ وظیفه تقســیم می‌کند. شــکل ۲ نشان‌دهنده یک تاثیر ســاده از این جابجایی فرد بین وظیفه‌های محوله اســت. هر قطعه از الگو، نشــان‌دهنده زمانی اســت که بر روی یک وظیفه متفاوت صرف شــده است. پیکان رو به پایین نشــان‌دهنده اولین زمانی است که پروژه بابت یک وظیفه تکمیل شــده ارزش دریافت می‌کند. در عمل، و به دلیل زمان تلف شــده برای جابجایی بین وظیفه‌ها، تاخیر بسیار بیش از این خواهد بود.

تصور کنید پروژه دیگری دارای وظیفه‌های مشــابهی است ولی فرد بر روی یک وظیفه تا زمان اتمام آن متمرکز می‌شــود. پروژه، همان‌گونه که در شــکل ۱ نشان داده شده، بسیار زودتر خلق ارزش خواهد کرد. تا زمانی که فرد یک وظیفه را کامل می‌کند، فرد متمرکز ســه وظیفه را تمــام کرده اســت: A،B و C. علاوه بر آن، وظیفه D را هم شــروع کرده است.

علیرغم این شــواهد، گاهی مشاهده می‌شود که فرد به دو یا سه پروژه اختصاص داده می‌شود. مدیران هم از این افراد انتظار دارند که هر کدام بخش مفیدی از وقت خود را مصروف هر پروژه کنند. در عمــل، نیازمندی اغلب پروژه‌ها دقیقــاً در ۲۵٪، ۴۵٪ یا ۷۵٪ یک هفته نمی‌گنجد. بدترین حالت این اســت که انتظار داشــته باشــیم افراد روزانه بین هر پروژه اختصاص یافته جابجایی داشته باشد.

در اغلــب محیط‌های کاری، افراد واقعاً ۸ ســاعت کامل از روز را روی یــک پروژه کار نمی‌کنند. طی کنفرانســی در ســال ۲۰۰۳، فردی از موسســه مهندســی نرم‌افزار[3] گزارش داد که بر اســاس بررسی ۲۰۰ پــروژه، میانگین زمان صرف شــده بر روی کار (منظور کاری اســت کــه در طرح پروژه به طور مشــخص تعیین و اختصــاص یافته)، ۱۵ ســاعت در هفته است؛ یعنی سه ســاعت در روز. یک فرد واقعاً چقدر می‌تواند در ۴۵ دقیقه (۲۵٪ از ســه ســاعت) از روز دســتاورد داشته باشد؟ بزرگترین بخش به همان اولویت تعریف شده اختصاص می‌یابد و هر چیز دیگری از سر باز شده و در اضافه کاری، موقعی که بهره‌وری در حالت کمینه است، انجام می‌شود.

مدیــران بزرگ به این موضوع واقف هســتند و کار (یا افرادی که یک بــه‌کار اختصــاص یافته‌اند) را به یک پروژه یا بــه دو کاری که تقریباً شبیه هستند، اختصاص می‌دهند. مدیران بزرگ به درستی دریافته‌اند که اگر آن‌ها یک پروژه مهم را قبل از شروع کار دیگری تحویل دهند، زودتر برای کسب‌وکار خلق ارزش کرده‌اند.

۵- افراد را مطلع نگهدارید

افــراد زمانی به بهترین نحــو کار می‌کنند که اطلاعــات مورد نیاز را داشته باشند. مدیران بزرگ دانسته‌های خود را درباره کار و نقش آن در اهداف پروژه یا سازمان با دیگران به اشتراک می‌گذارند.

اگر چه افراد نیازمند داشــتن اطلاعات درباره کارهای خود هســتند، ولی نیاز دارند تا از تصویر کلی[4] پروژه هم اطلاعاتی داشــته باشــند.

3- Software Engineering Institute (SEI)

4- Big Picture

مدیــران ضعیف اطلاعات را کم‌کم و حســب نیاز فرد، ارائه می‌دهند. مدیران بزرگ اطلاعاتی را در خصوص کارها به طور خاص ارائه داده، ضمــن آن‌که توضیــح می‌دهند جایگاه ایــن کار در ماموریت گروه و موفقیت شــرکت کجا اســت. این‌که فرد (مدیر) قادر باشد کار را در قالب یک تصویر بزرگتر ارائه کند، می‌تواند در افراد ایجاد انگیزه کرده و به تصمیم‌گیری بهتر آن‌ها کمک کند.

با مدیری ملاقات داشتم که طرح کلی پروژه را نزد خود نگه می‌داشت و به افراد اجازه می‌داد فقط کارهای خود را مشاهده کنند. به همین دلیل، افرد مجبور بودند به نحوی به طرح کلی پروژه دست پیدا کنند یا بدانند چه افرادی به‌کارهای آن‌ها وابسته هستند، از چه کسی باید ورودی بگیرند و قرار است کجا با دیگران همکاری داشته باشند. این مدیر، فرصت این‌که افراد کار خود را در یک افق گســترده‌تر دیده و امکان اثربخشی و همکاری با دیگران را داشته باشند، از آن‌ها گرفت. این کار او این گونه تفسیر شد که او به افراد اعتماد نداشته و آن‌ها را به شــکل «واحدهای بیولوژیکی مولد کد» می‌بیند، تا افراد باهوش و خلاقی که قادرند کارهای خود را طرح‌ریزی و مدیریت کنند.

افراد نیازمند داشتن اطلاعاتی درباره کار خود هستند. آن‌ها همچنین نیازمند اطلاعاتی درباره وقایع و اولویت‌های ســازمان خود هســتند. هنگامی که افراد با خلأ فقدان این اطلاعات مواجه می‌شــوند، آن‌را با بدترین نوع ترس و شایعه پر می‌کنند. شایعه و برداشت‌های سطحی، وقت بســیار زیادی را از مدیریت در سازمان‌ها می‌گیرد. بدون افشای اطلاعات شخصی افراد یا عدول از چارچوب‌های قراردادی، هرآنچه را که می‌تواند به اشتراک گذاشــته، اطلاع‌رسانی کنید. اگر موضوعی را نمی‌دانید، آن را پذیرفته و هنگامی که دانستید، اطلاع‌رسانی کنید.

مدیران هم باید از موضوعاتی مانند وضعیت، موانع یا دغدغه‌ها (افراد و پروژه) آگاه باشــند. برگزاری نشســت‌های منظم برای ارائه گزارش وضعیــت پروژه (از نوعی که در آن افراد تک‌تک به مدیر خود گزارش می‌دهنــد)، اگرچه در زمان مدیر صرفه‌جویی می‌کند، ولی وقت افراد دیگر را تلف می‌کند. نوعاً این افراد فقط بخشی از اطلاعاتی را که برای دانســتن مدیر نیاز است، بیان می‌کنند. بسیاری از موضوعات مهم در این نوع جلســات ناگفته می‌ماند. بــه عنوان مثال، افراد اغلب به جای این‌که بپذیرند مجادله می‌کنند. موانع، مشکلات را آشکار می‌کنند یا در یک جمع گروهی از آرمان‌های حرفه‌ای خود صحبت می‌کنند. این همان اطلاعاتی اســت که یک مدیر بزرگ نیازمند دانســتن آن است. جلســات نفر-به-نفر را با هدف آشنایی با بخش شخصی کار و ارتباط دائــم با اهداف حرفه‌ای آن‌هــا، برگزار کنید. جلســات تیمی را برای کارهای وابســته به هم، حل مشکل به شکل گروهی یا تصمیم‌گیری تیمی نگهدارید.

۶- بازخورد بدهید

افــراد نیاز دارند بداننــد کارهای خود را چگونه انجــام می‌دهند. این تصــور که افراد می‌دانند کی از کارها عقب افتاده‌اند یا چه کارهایی را به خوبی انجام می‌دهند، نادرست است. مدیران بزرگ با تک‌تک افراد به شــکل منظم هفتگی یا یک هفته در میان جلســه دارند؛ هدف از برگزاری این جلســات ایجاد فرصتی برای ارائه بازخورد به افراد برای اصلاح روش و عملکرد آن‌ها اســت. این جلســات همچنین فرصتی را برای توجه و قدردانی از مواردی که مرتبط با مشــارکت و حضور فرد است، فراهم می‌کند.

بازخوردهای خاص فردی ارائه کنید تا افراد بر اساس آن اقدام کنند. با خانمی صحبت می‌کردم که رئیسش به او گفته بود او خیلی خوب است. او درمانــده بود که چه کار باید بکند؟ بازخورد مناســب، توصیف‌کننده رفتار یا وضعیت اســت و نیز بیان‌کننده اثــرات این رفتار؛ هنگامی که خواسته باشید فرد رفتار خود را عوض کرده یا همان را ادامه دهد.

من این ساختار را برای ارائه بازخوردهای اثربخش پیشنهاد می‌کنم:

۱) با یک مقدمه شروع کنید.

۲) رفتار یا نتیجه را توصیف کنید.

۳) اثرات آن را بیان کنید.

۴) درخواســت خود را ارائه داده یا او را درگیر حل مســئله به‌صورت مشترک کنید.

آنچه در ادامه می‌آید، مثالی اســت که یک مدیر خوب ممکن است به آن خانم خوب گفته باشد:

۱) چیزهای را مشــاهده کردم ممکن اســت برای شما مفید باشد. آیا زمان مناسبی برای صحبت کردن است؟

۲) در جلسه امروز متوجه شدم که شما با همه درخواست‌های بخش بازاریابی برای تغییر در ویژگی‌های محصول موافقت کردید.

۳) می‌دانم که اضافه‌کاری شــما زیاد است و یک فهرست طولانی هم از کارهای در دســت انجــام دارید. چیزی که می‌بینم این اســت که شــما قدرت نقد بخش بازاریابی را از دســت داده‌اید، به این دلیل که موافق انجام کارهایی هســتید که در چارچوب‌های زمانی مورد انتظار بازاریابی محقق نمی‌شود.

۴) اجــازه بدهید درباره چگونگی مدیریــت انتظارات و انجام کارهای بااهمیت، بدون این‌که شما خسته و مستاصل شوید، صحبت کنیم.

مدیــران بزرگ تا مرور گزارش ســالانه بــرای ارائه بازخــورد منتظر نمی‌ماننــد، این نــوش‌دارو بعد از مرگ ســهراب اســت. اگر خواهان موفقیت کسی هستید، هرچه سریع‌تر آنچه را نیاز به تغییر دارد به او بگویید، تا امکان اصلاح خود را داشــته باشد. دلیلی ندارد اجازه دهید ناکارآمدی یا اشتباهات تکرار شوند؛ این فقط بهره‌وری و روحیه افراد و تیم را کاهش داده و تضعیف می‌کند.

۷- افراد را ارتقاء دهید

مدیــران بزرگ از آرمان‌های شــغلی و حرفه‌ای افرادی که با آن‌ها کار می‌کنند، آگاهی داشــته و به همین دلیل تلاش می‌کنند هر

زمـان کـه بتوانند در دسـتیابی اهداف به آن‌ها کمـک کنند؛ به حرکت افرادی هم که نمی‌توانند در این مسیر گام بردارند، کمک می‌کنند.

کارمند باسـابقه یک شـرکت، می‌خواسـت از بخش آزمون به توسعه منتقل شـود. او تا آنجا که می‌توانسـت کارهای فنـی زیادی مربوط بـه آزمون انجـام داد و حتی در وقت‌های آزاد خودش برنامه‌نویسـی را هم مطالعه کرد. از آنجا که می‌دانسـت چگونـه باید کد را بخواند، سـرمایه‌ای برای تیم در نحوه طراحی آزمون‌هایی که وابسـته به یک واسطه گرافیکی بودند، محسوب می‌شد.

هنگامی که این فرد درخواسـت خود را برای یک موقعیت شـغلی در تیم برنامه‌نویسـی به رییس خود ارائه داد، با مخالفت او مواجهه شد. رییس عقیده داشـت: «شـما اینجا فردی بسـیار ارزشمند هستید.» کارمند ظرف کمتر از یک ماه از آن شرکت رفت و در شرکت دیگری به عنوان برنامه‌نویس اسـتخدام شد؛ نتیجه این شد که تیم و شرکت یک کارمند با ارزش را از دست دادند.

مدیـران بزرگ با افـراد در خصوص مهارت‌هایی که دوسـت دارند داشـته باشـند و مسـیری کـه باید بـرای تحقق آن طـی کنند، صحبت می‌کنند. این مدیـران فرصت‌هایی را برای ایجاد مهارت‌ها و ظرفیت‌هـا در کار روزانـه پیدا می‌کنند. قصد کسـب یک مهارت جدید، اغلب قربانی مهلت‌های فشرده زمانی پروژه است؛ مگر این‌که در کارهـای روزانه فرد برنامه‌ریزی شـده باشـد. یافتن فرصت‌های ارتقـاء در برنامه کارهـای روزانه، هم مهارت ایجـاد می‌کند و هم وفـاداری. حتی هنگامی که افراد پیشـرفت می‌کنند، مدیرانی را به یـاد می‌آورند که روی آن‌ها سـرمایه‌گذاری کردند؛ نه فقط از توان کاری آن‌ها استفاده کردند.

در شـرکت دیگـری، آزمون‌گری می‌خواسـت به سـمت مدیریت پروژه‌های آزمون (راهبر آزمون) منتقل شود. مهلت‌های زمانی پروژه به نحوی بود که فرستادن یک آزمون‌گر به سمیناری خارج از محل اجرای پروژه، امکان‌پذیر نبود. ولی او و مدیرش یک کتابخانه کوچک از کتاب‌هـا و مقالات را برای مطالعه آزمون‌گر پیدا کردند. مدیر هم روش مطالعـه کتاب و اجرای آن را به عنوان یک «پرونده کوچک» به آزمون‌گر آمـوزش داد. مدیر به آزمون‌گر یاد داد تا کارهای خود را بـه بخش‌هـای یک یا دو روزه تقسـیم کـرده و معیارهای پایان هر بخـش را تعریف کند. مدیـر به این مدیر پروژه تازه‌کار نشـان داد چگونه می‌تواند پیشـرفت خود را اندازه‌گیری کرده و در زمانی کـه این میزان رضایت‌بخش نبود، بـا او در انتخاب راهکارهای رفع مشـکل همفکری می‌کرد. در پایان پروژه، هم آزمون‌گر و هم مدیر از انتصاب آزمون‌گر به سـمت رهبر آزمون احساس خوبی داشتند، جایی که او می‌توانسـت کار خود و دو نفر دیگر از همکاران خود را ساماندهی و ردیابی کند.

برعکـس، هنگامی که مدیران بزرگ کاری که مهارت‌های جدیدی را ایجاد می‌کنند ندارند، مسـتقیم با افراد صحبت می‌کنند. سال‌ها قبل بـا مرد جوانـی صحبت می‌کـردم که می‌خواسـت از بخش برنامه‌نویسـی رایانه‌های بزرگ[5] به بخش برنامه‌نویسـی رایانه‌های شخصی[6] منتقل شود. می‌دانستم که کار در گروه ما به او در رسیدن بـه این هدف کمکی نخواهد کـرد. به جای تلاش برای ممانعت او، مقدمه‌ای کوتاه از شرکت برای او بیان کردم. بعدها، وقتی او به یک واحد دیگر منتقل شـده و توانسـت کار دلخواه خود را ادامه دهد، مرا به یک ناهار دعوت کرد. ضمن ناهار، گفت: «شـما با من صادق بودید». «من در خصوص ترک گروه احسـاس بدی داشتم، ولی از شما سپاسگزارم که تلاشی نکردید خارج از آنچه می‌خواستم با من صحبت کنید.» او همچنین بعدها اسـتخدام‌کننده خوبی برای من شد.

بـرای ارتقاء افـراد، نیاز به بودجـه کلانی ندارید. به دنبـال راه‌هایی بـرای توسـعه مهارت‌های حوزه‌ای حتـی در کارهای روزانه باشـید. روش افزایش زیرکی سـازمانی را فرا گیرید و برای ایجاد مهارت‌های مدیریتـی، تفویض اختیار کنیـد. این یکی از بهتریـن روش‌ها برای نگهداشـت با ارزش‌ترین کارمندان است؛ برای شـما و برای سازمان شما.

۸- جمع بندی

مدیریـت کار سـاده‌ای نیسـت، ولی دور از دسـترس هم نیسـت. شـیوه‌های گفته شده در بالا را به شکل سـازگار و مستمری به‌کار ببندید؛ شـما واقعاً در مسیر بدل شدن به یک مدیر بزرگ خواهید بـود. از کارهای دیگـران با تمرکز بـر روی اولویت‌بنـدی کارها و توانمندسـازی بهره‌وری بهره خواهید برد. به رشـد و ارتقاء افراد از طریق کمک به آن‌ها در مشـاهده کار خودشـان در حوزه کاری و اصـلاح کارها و نیز فراهم کردن فرصت‌های جدید برای توسـعه و ظرفیت کمک کنید. و بهتر از همه این‌که، شما هم در نزد مدیرتان خوب به نظر خواهید رسید.

۹- قدردانی

از سـرکار خانـم نرگـس عظیمـی که زحمـت تهیه و آماده‌سـازی پیش‌نویس این مقاله را متقبل شدند، سپاسگزاری می‌کنم.

۱۰- منبع

این مقاله از منبع زیر برگرفته شده است:

* Esther Derby, Becoming a Great Manager: Five Pragmatic Practices, CrossTalk, November 2006, pp. 9-11.

5- Mainframes

6- Personal Computers (PCs)

تحلیل جامع نیازمندی‌های امنیتی در سیستم‌های اجتماعی- فنی

فاطمه قربانی

دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات گرایش معماری سازمانی، آزمایشگاه معماری سازمانی، دانشگاه صنعتی شیراز

پست الکترونیکی: f.ghorbani88@gmail.com

سیدرئوف خیامی

هیئت علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات، آزمایشگاه معماری سازمانی، دانشگاه صنعتی شیراز

پست الکترونیکی: khayami@sutech.ac.ir

چکیده

امنیت برای سازمان‌های بزرگ به‌ویژه موسسات مالی و دولتی نگرانی فزاینده‌ای است، زیرا نقض امنیت در سیستم‌های وابسته به آن‌ها بارها منجر به زیان میلیاردها دلار در سال شده است و این هزینه در حال افزایش است. دلیل اصلی این نقض‌های امنیتی، اجتماعی- فنی بودن سیستم‌های موردنظر هستند. سیستم‌های اجتماعی- فنی سیستم‌هایی هستند که در آن‌ها ترکیبی از افراد، فرآیندها، فناوری و زیرساخت مشاهده می‌شود. این در حالی است که به جای استفاده از روش طراحی جامع، این‌گونه سیستم‌ها به‌صورت جزئی طراحی می‌شوند، از این رو بخشی از سیستم آسیب پذیر باقی می‌ماند. یکی از کارهایی که برای مقابله با این مشکل انجام شده پیشنهاد یک چارچوب سه لایه برای تحلیل امنیت در این‌گونه سیستم‌ها است. این چارچوب در سال ۲۰۱۶ توسط تانگ لی و همکارانش معرفی شد. لایه اجتماعی (فرآیندهای کسب‌وکار، عامل‌های اجتماعی)، لایه نرم‌افزار (برنامه‌های نرم‌افزاری که از لایه اجتماعی پشتیبانی می‌کنند) و لایه زیرساخت (زیرساخت فنی و فیزیکی) لایه‌های تشکیل‌دهندهٔ این چارچوب هستند. در این طرح پیشنهادی، نیازمندی‌های سراسری امنیت منجر به نیازمندی‌های امنیتی محلی شده، تحلیل امنیتی لایه بالایی تجزیه و تحلیل لایه‌های پایین‌تر را تحت تاثیر قرار می‌دهد. تانگ لی و همکارانش در کنار این چارچوب، مجموعه‌ای از روش‌های تحلیلی و یک فرآیند سیستماتیک نیز معرفی کردند که در کنار هم تحلیل نیازمندی‌های امنیتی در این سه لایه را هدایت می‌کنند. همچنین در این چارچوب برای مقابله با پیچیدگی سیستم‌ها مجموعه‌ای از قواعد استنتاجی تعریف شده است که تحلیل را خودکار یا نیمه خودکار می‌سازند. فرآیند تحلیل در یک ابزار نیز پیاده‌سازی شده است.

واژه‌های کلیدی: الزامات امنیتی، مدل هدف، معماری سازمانی، سیستم اجتماعی- فنی، الگوی امنیت

مقدمه

سیستم‌های اجتماعی- فنی (STS) سیستم‌های سازمانی هستند که از افراد، فرآیندهای کسب‌وکار، نرم‌افزارها و مولفه‌های سخت‌افزاری تشکیل می‌شوند. این‌گونه سیستم‌ها معمولا دارای یک زیرساخت فیزیکی غنی هستند که نه تنها شامل کامپیوترهاست بلکه ساختمان‌ها، شبکه‌های کابلی و مانند این را نیز در برمی‌گیرد. در

اثـر پیچیدگـی روزافزون سیسـتم‌های STS، این سیسـتم‌ها به‌طور فزاینده‌ای شـکاف امنیتی را تجربه می‌کنند، شکاف‌هایی که ناشی از نقص و آسیب‌پذیری‌های امنیتی هستند.
ریشـهٔ معمول بسـیاری از ایـن شـکاف‌های امنیتی این اسـت که راه‌حل‌هـای امنیتی به روشـی جامع طراحی نمی‌شـوند. در عوض با روشـی جزئی بـه آن‌ها پرداخته می‌شـود؛ تحلیل‌گـران مختلف، در زمان‌های مختلف و با اسـتفاده از تکنیک‌هـای تحلیلی متفاوت تنها روی یـک لایـه مفهومی از سیسـتم تمرکز می‌کنند. بـدون در نظر گرفتـن تعاملات میان لایه‌های مختلف یک سیسـتم، تحلیل امنیتی جزئی منجر به شکاف و آسیب‌پذیری بخش‌هایی از یک سیستم STS می‌شود در حالی که سایر بخش‌ها ممکن است تحت محافظت باشند. برای رفع این مشکل تانگ لی و همکارانش چارچوبی را پیشنهاد کردند که نیازمندی‌های امنیتی STS ها را براساس نیازمندی‌های عملکردی سیسـتم و به روشـی جامع مورد تجزیه و تحلیل قـرار می‌دهد. این چارچوب از سـه لایه تشکیل شده اسـت: لایه اجتماعی (فرآیندهای کسـب‌وکار، عامل‌های اجتماعی)، لایه نرم‌افزار (برنامه‌های نرم‌افزاری که از لایه اجتماعی پشتیبانی می‌کنند) و لایه زیرساخت (زیرساخت فنـی و فیزیکی). هر لایـه روی نگرانی‌های خاصی متمرکز اسـت و نیازمندی‌هـا و مشـخصات مربوط به خـودش را دارد. نیازمندی‌ها و مشـخصات هر لایه از طریق مدل‌های نیازمندی هدف محور به دست می‌آیند. مشـخصات یک لایه نیازمندی‌های لایه پایین‌تر را مشخص می‌کند و این‌گونه وابستگی‌ها با پیوندهای میان لایه‌ای ثبت می‌شوند. در نتیجه چارچوب پیشنهادی نه تنها در هر سه لایه تحلیل نیازمندی را انجـام می‌دهـد بلکه وابسـتگی‌های متقابل لایه‌هـا را نیز در نظر می‌گیـرد. به‌عنوان خروجی نهایی، راه‌حل‌هـای امنیتی جامعی تولید می‌شـود که این راه‌حل‌ها می‌توانند نیازمندی‌هـای امنیتی در تمام لایه‌ها را برآورده نموده و محافظت امنیتی جامعی را فراهم نمایند.
توسـعه دهندگان این چارچوب برای تحلیـل امنیتی درون لایه‌ای و میان لایه‌ای یک فرآیند سیسـتماتیک معرفی کردند. در این فرآیند نیازمندی‌های عملکردی سیسـتم و نیازمندی‌های امنیتی سطح بالا به‌عنوان ورودی گرفته می‌شـود، سپس تحلیل نیازمندی‌های امنیتی در سراسر این سه لایه تکرار می‌شود تا راه‌حل‌های جامع تولید شوند. بـرای آن‌کـه تحلیل‌ها نیاز به دانش امنیتی زیادی نداشـته باشـند، مجموعه‌ای از قواعد استنتاجی فرمال نیز ارائه شده است.

۱- مبانی اولیه

قبـل از آن‌که به معرفی چارچوب و نحوهٔ عملکرد آن پرداخته شـود لازم است مفاهیمی که مبانی اولیهٔ شکل‌گیری این چارچوب می‌باشند تعریف شوند. مسئله نیازمندی، که کارهای اصلی در تحلیل نیازمندی را مشخص می‌سـازد، زبان مدل‌سازی نیازمندی‌ها و الگوهای امنیتی که بـرای عملیاتی کردن نیازمندی‌های امنیتی موردنیاز هسـتند، از جملهٔ این مفاهیم می‌باشـند که در ادامه هریـک از آن‌ها به اختصار شرح داده می‌شوند.

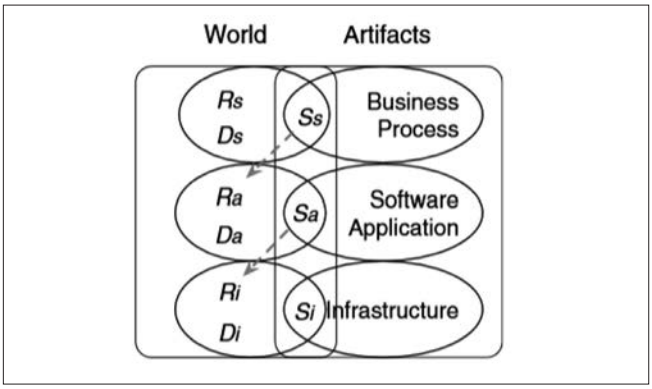
۱-۱- مسئله نیازمندی‌ها

یک مسئله نیازمندی از سه مفهوم تشکیل شده است:
نیازمندی (Requirement): یک ویژگی مورد تقاضا که مشخص‌کنندهٔ نیازهای سـودبران بوده و انتظار می‌رود که سیستم مطلوب (to-be) آن‌ها را برآورده سازد.
فرض دامنه (Domain Assumption): یک ویژگی دلالت کننده که به سیستم مطلوب مربوط می‌شود.
مشخصات (Specification): یک ویژگی مورد تقاضا که برای برآورده کردن نیازهای سـودبران به‌صورت مسـتقیم توسط سیستم مطلوب پیاده‌سازی می‌شود.
براسـاس این سه مفهوم، مسـئله نیازمندی می‌خواهد مشخصهٔ S را پیدا کند که بتواند تحت فرضیات دامنه D نیازمندی‌های داده شـده R را برآورده سازد. بنابراین مسئله نیازمندی به‌صورت D ,S|-R نشان داده می‌شـود، به این معنا که نیازمندی‌ها مسـتلزم فرضیات دامنه و مشخصات در کنار یکدیگر هستند.

۱-۲- مدل‌های نیازمندی مبتنی بر هدف

مهندسـی مبتنی بر هدف نیازمندی‌ها یـک ابزار جدید برای دریافت و ثبت اهداف سـودبران و درک انگیزه‌های اصلی برای نیازمندی‌های عملکـردی و غیرعملکردی اسـت. زبان‌های مدل‌سـازی هدف محور (مثل *i و Tropos)، تکنیک‌های تحلیل و مدل‌سـازی ارائه می‌دهند که برای تحلیل جامع نیازمندی‌های امنیتی در این چارچوب نیز مورد اسـتفاده قرار گرفته‌انـد. در این کار برای مدل‌سـازی نیازمندی‌های عملکـردی و غیرعملکردی (در حوزهٔ امنیت) پایهٔ مدل‌های سـه لایه روی ترکیبی از این روش‌ها قرار داده شده است. به‌طور خاص مفاهیم و روابط زیر از *i و Techne گرفته شده است:

- goal: وضعیت دلخواه یک actor با معیارهای تحقق مشخص.
- softgoal: مشـابه با goal با این تفاوت کـه معیارهای تحقق آن مشخص نیستند.
- task: نشـان‌دهندهٔ عملی اسـت که توسـط یـک actor و برای دستیابی به برخی از اهداف انجام می‌شود.
- resource: یـک موجودیت (فیزیکی یا اطلاعاتی) که actor برای انجام یک task به آن نیاز دارد.
- Domain assumption: یـک ویژگـی دلالت‌کنندهٔ یک دامنه را نشان می‌دهد.
- رابطـه refinement: یک رابطه عام که سـاختار سلسـله مراتبی عناصر نیازمندی‌ها (مثل goal و task) را نشان می‌دهد. به‌طور خاص دو نوع refinement وجود دارد: refine(-or) و and-refine. برای اولین نـوع، برآورده نمودن حداقل یک گـره فرزند می‌تواند گره پدر را محقـق سـازد، در حالی که برای دومین نوع، بـرآورده کردن تمام



شکل ۱: مسئله نیازمندی تعمیم داده شده برای سیستم STS

گره‌های فرزند برای تحقق گره پدر لازم است.

• رابطه dependency: یک رابطه اجتماعی میان دو actor را نشان می‌دهد.

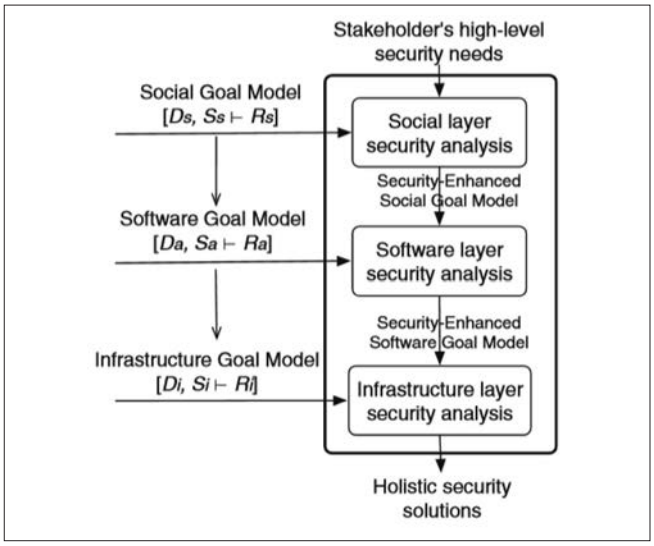
• رابطه contribution: تاثیر یک goal/task روی یک softgoal را نشان می‌دهد و به تحلیل‌گر در تصمیم‌گیری میان چندین goal و task کمک می‌کند.

۱-۳- الگوهای امنیتی

الگوهای امنیتی از جفت «نیازمندی امنیتی (مسئله)، سازوکار امنیتی (راه‌حل)» تشکیل شده‌اند و یک روش خاص برای حل یک مسئله امنیتی را بیان می‌کند. این الگوها دانش امنیتی را به‌صورت کپسوله در اختیار تحلیل‌گران قرار می‌دهند و از این طریق نیاز به تخصص امنیتی را کاهش می‌دهند. الگوهای امنیتی متعددی ارائه شده‌اند که سطوح انتزاعی متفاوتی را پوشش می‌دهند. علاوه بر الگوهای منفرد، تعدادی مخزن نیز وجود دارند که الگوهای موجود در پژوهش‌ها را جمع‌آوری کرده‌اند. در توسعهٔ این چارچوب از الگوهای امنیتی استفاده شده است تا اهداف امنیتی به کمک سازوکارهای امنیتی در هر سه لایه عملیاتی شوند. در این راستا از منابع دانش مختلفی برای هر سه لایه استفاده شد که به ترتیب عبارتند از: الگوهای امنیت سازمانی، الگوهای امنیت نرم‌افزار، الگوهای امنیت فیزیکی. از آنجایی که تعداد کمی الگوی امنیت فیزیکی وجود دارد، ISO 27002 نیز به‌عنوان یک مکمل برای این لایه به‌کار گرفته شد.

۳- چارچوب سه لایه تحلیل امنیت

سیستم‌های STS در مقایسه با سیستم‌های نرم‌افزاری سنتی تعداد زیادی آرتیفکت دارند که برای موثر بودن کار کل سیستم توجه به آن‌ها لازم و ضروری است. در توسعهٔ این چارچوب در واقع روی سه جنبهٔ مهم STS که بیشترین توجه جامعهٔ امنیت معطوف به آن‌هاست تمرکز شده است و آن‌ها را در سه لایه سازماندهی کرده‌اند. در انتزاعی‌ترین سطح، یک لایه اجتماعی از نظر عامل‌های اجتماعی، وابستگی‌های اجتماعی و فرآیندهای کسب‌وکار مفهوم‌سازی شده



شکل ۲: نمای کلی چارچوب تحلیل سه لایه

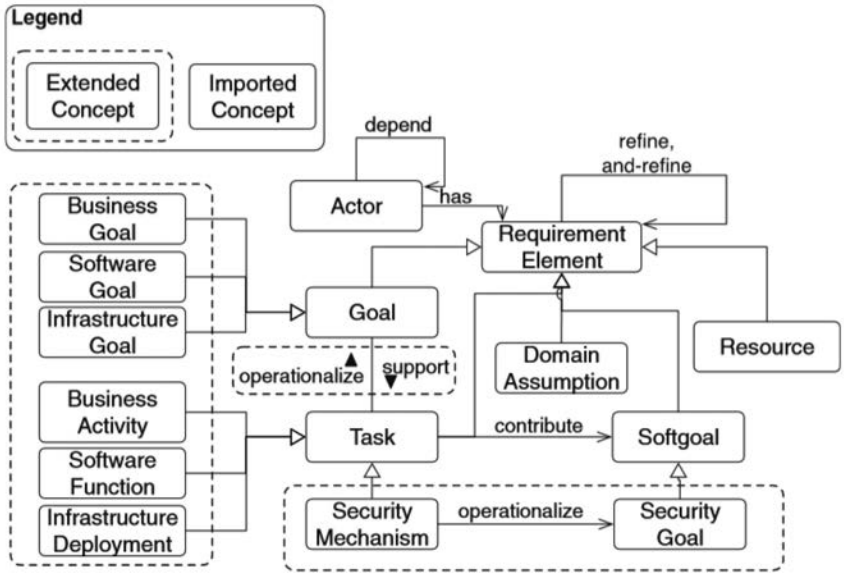
است. در لایه بعد نرم‌افزارهایی که از لایه اجتماعی پشتیبانی می‌کنند مورد توجه قرار گرفته‌اند. در آخر، یک لایه زیرساخت، که روی زیرساخت فنی و فیزیکی متمرکز بوده و از توسعهٔ نرم‌افزارها و فرآیندهای کسب‌وکار پشتیبانی می‌کند، در نظر گرفته شده است.

هر لایه نیازمندی‌های مختص به خودش را دارد که از طریق مشخصات خاص لایه و تحت فرضیات دامنه متناظر برآورده می‌شود. همان‌طور که در شکل ۱ نشان داده شده است مشخصات یک لایه، تعیین کنندهٔ نیازمندی‌های لایه‌های پایین‌تر است. معنا و مفهوم این وابستگی‌ها این است که دستیابی به مشخصات یک لایه نیازمند برآورده کردن نیازمندی‌ها در لایه پایین‌تر است.

شکل ۲ ساختار کلی این چارچوب سه لایه را نشان می‌دهد و همان‌طور که مشخص است چارچوب کار خود را با نیازمندی‌های سودبران شروع نموده و آن‌ها را در هر سه لایه و با توجه به اهداف و مشخصات خاص هر لایه تجزیه و تحلیل می‌نماید. حاصل این فرآیند مجموعه‌ای از راه‌حل‌های جامع امنیتی است که هر سه لایه را در برمی‌گیرند.

مدل‌هایی که برای ضبط مشخصات و نیازمندی‌ها در هریک از لایه‌ها ارائه شده‌اند از دو دسته مفهوم تشکیل می‌شوند. دسته اول مفاهیمی هستند که با توجه به زبان‌های مدل‌سازی تعریف می‌شوند و در بخش قبل معرفی شدند و دسته دوم مفاهیم جدیدی هستند که خاص این مدل‌ها تعریف می‌شوند. شکل ۳ نمای کلی فرامدل پیشنهادی این چارچوب را نشان می‌دهد. در این شکل مفاهیم جدید با نقطه چین مشخص شده‌اند.

باید توجه داشت که این چارچوب softgoal ها و پیوندهای مشارکتی غیرامنیتی را در بر نمی‌گیرد و منحصرا متمرکز بر تحلیل نیازمندی‌های امنیتی است، اگرچه می‌توان آن را به راحتی برای نیازمندی‌های غیرامنیتی نیز گسترش و تعمیم داد.



شکل ۳: فرامدل چارچوب سه لایه تحلیل نیازمندی‌های امنیتی

شـکل ۴ بخشی از مدل سـه لایهٔ نیازمندی‌ها را برای یک سناریوی شبکه هوشمند نشـان می‌دهد. از این فرانامه (سناریو) و مدل جزئی آن برای نشـان دادن بهتر مدل‌سازی سه لایه نیازمندی‌ها در STS و مفاهیم مرتبط استفاده می‌شود.

۲-۱- مفاهیم تعمیم داده شده نیازمندی

از آن جایـی کـه مدل‌های هدف برای لایه‌هـای مختلف و به منظور توجه به نگرانی‌های متفاوت سـاخته می‌شوند، Goal به اهداف خاص لایه تقسـیم می‌شـود و روی جنبه‌های خاصی از نیازهای سـودبران تمرکز خواهد داشت.

- Business Goal: نیازمندی‌های سـطح بالای سـودبران در حوزهٔ کسب‌وکار (BG1 در شکل ۴)
- Software Goal: نیازمندی‌های سودبران در ارتباط با نرم‌افزارهایی که از فعالیت‌های تجاری متناظر پشتیبانی می‌کنند (AG1 در شکل ۴)
- Infrastructure Goal: نیازمندی‌هـای سـودبران بـا توجـه به زیرسـاخت فنی و فیزیکی که از اجرای نرم‌افزارها پشـتیبانی می‌کند (IG2 در شکل ۴).

برهمین اسـاس Task ها نیز در لایه‌های مختلف به تعاریف عملیاتی خاصی نسبت داده می‌شوند که منعکس کنندهٔ آن لایه است.

Task در لایه اجتماعی یـک فعالیت تجاری (Business Activity)، در لایـه نرم‌افزار یک تابع نرم‌افـزاری (Software Function) و در لایه زیرساخت یک تنظیم استقرار (Deployment Setting) است.

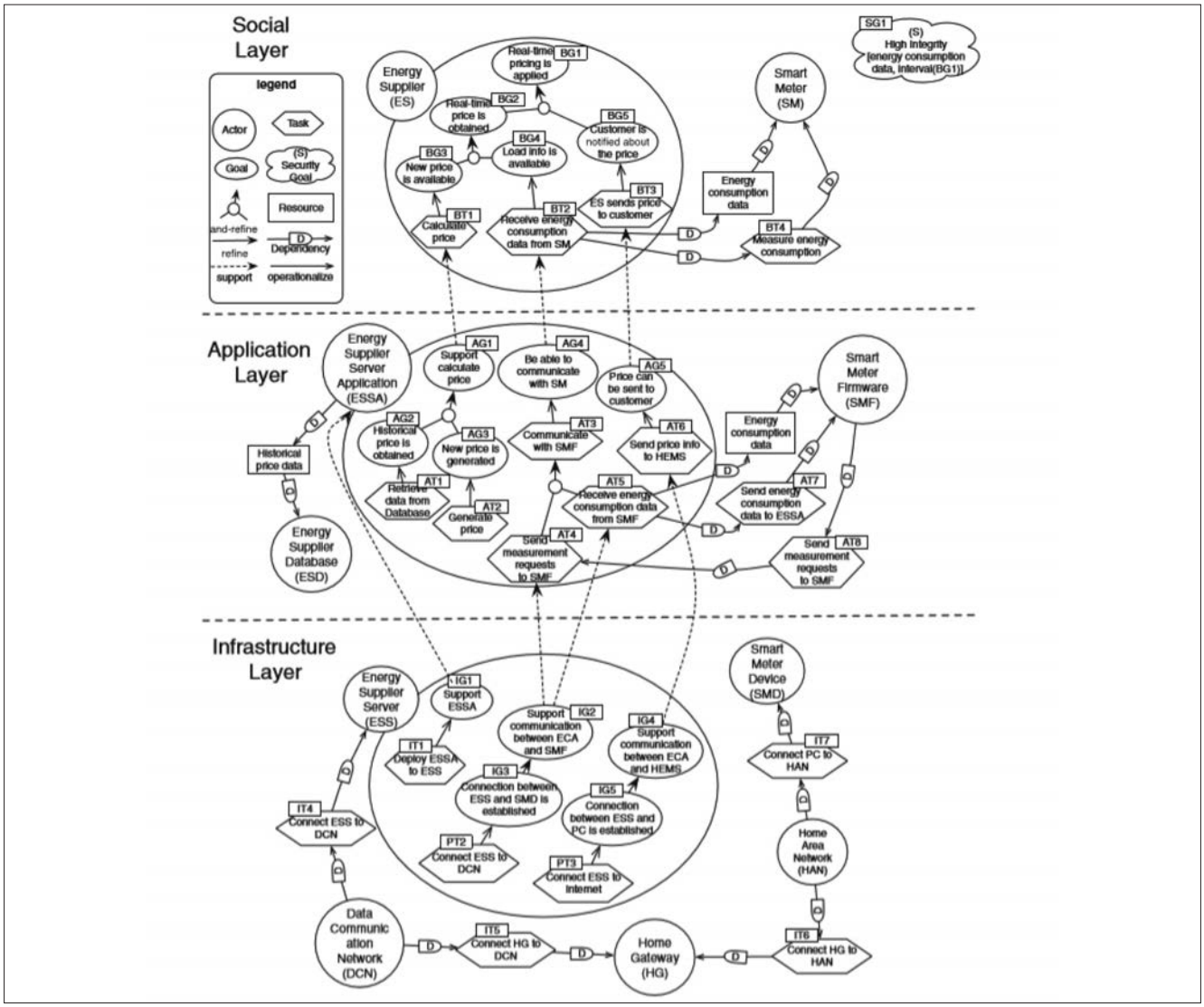
باید توجه داشـت که هنگام شناسـایی و مدل‌سازی Taskها در لایه اجتماعـی، تحلیل‌گران باید تنها روی پدیده‌هـای خاص لایه تمرکز داشـته باشـند و نگرانی‌های لایه پایین‌تر را نادیده بگیرند. به‌عبارت دیگـر تحلیل‌گر تنها بـه فعالیت‌های تجاری توجـه می‌کند که برای دستیابی به هدف کسب‌وکار موردنیاز می‌باشند، صرف نظر از این که از نرم‌افزاری در این فعالیت‌ها استفاده می‌شود یا خیر و چگونه.

علاوه بـر مفاهیم فوق دو رابطـهٔ دیگر نیز در چارچوب پیشـنهادی گنجانده شده است:

- Operationalize: یـک goal را بـه task ای که آن هدف را درون همان لایه عملیاتی می‌کند مرتبط می‌سازد (BG5 با BT3 در شکل ۴).
- Support: یـک رابطهٔ میان لایه‌ای اسـت که نشـان می‌دهد یک goal در یـک لایـه از task در یـک لایه بالاتر پشـتیبانی می‌کند. بنابراین تکمیل شدن task نیازمند برآورده شدن goal است.

برای تعیین این که task نیازمند پشتیبانی از یک لایه پایین‌تر است یـا خیر، تحلیل‌گر باید تعریـف عملیاتی خاص لایهٔ آن task را مورد توجه قرار دهد. به‌طور خاص، از آن جایی که task در لایه اجتماعی یک فعالیت تجاری اسـت، تحلیل‌گر باید تعیین کند که آیا اجرای آن فعالیت به نرم‌افزاری نیاز دارد یا خیر و اگر نیاز داشت باید یک پیوند support اضافه شود (AG5 و BT3 در شکل ۴).

علاوه بر این، از آن جایی که در لایه کاربرد task یک تابع نرم‌افزاری اسـت به‌صـورت پیش فـرض این‌گونه taskهـا نیازمند پشـتیبانی سـخت‌افزار فیزیکی آن نرم‌افزار می‌باشـند. همان‌طور که در شکل ۴ نشان داده شده است برای مدیریت مسئلهٔ مقیاس‌پذیری، به جای این که برای هر task در لایه کاربرد پیوند support از لایه زیرسـاخت ایجاد شـود، آن را از infrastructure goal لایـه پایین‌تر به عامل کاربرد لایه بالاتر رسم می‌کنند (از IG1 به ESSA). از نظر مفهومی آن پیوند support نشان می‌دهد که تمام taskهای عامل کاربرد توسط هدف زیرسـاخت پشتیبانی می‌شـوند. علاوه بر این پیوند support پیش فـرض، تحلیل‌گر باید بـرای هر task کاربـرد (داخل یا خارج



شکل ۴: بخشی از مدل سه لایهٔ نیازمندی‌ها برای سناریوی شبکه هوشمند

عامل ESSA) مشخص کند که آیا task به پشتیبانی بیشتر از لایه زیرساخت نیاز دارد یا خیر (AT5 و IG3 در شکل ۴).

مفاهیم تعمیم داده شده نیازمندی امنیتی

• Security goal: نیازهای امنیتی سودبران باتوجه به دارایی و بازه زمانی. هدف امنیتی نوع ویژه‌ای از softgoal است که روی نگرانی‌های امنیتی تمرکز دارد.

اهداف امنیتی از لحاظ معنایی به goal/task ها متصل می‌شوند، این اتصال از طریق یک ویژگی داخلی برقرار می‌شود.

هر هدف امنیتی با الگوی زیر نشان داده می‌شود:

[<asset>,<interval>]<security property><importance

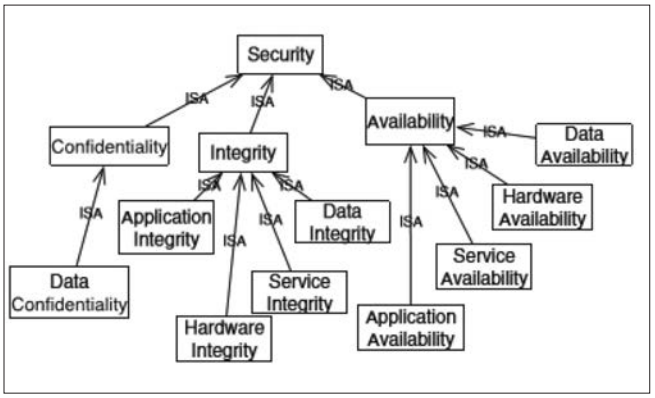
به‌عنوان مثال SG1 در شکل ۴ را در نظر بگیرید. این هدف امنیتی بیان می‌کند که نیازمندی امنیتی «حفاظت درجه بالا از یکپارچگی داده‌های مصرف انرژی در بازه زمانی اجرای BG1» موردنظر سودبران است.

هریک از پارامترهای الگوی فوق در زیر تعریف می‌شوند:

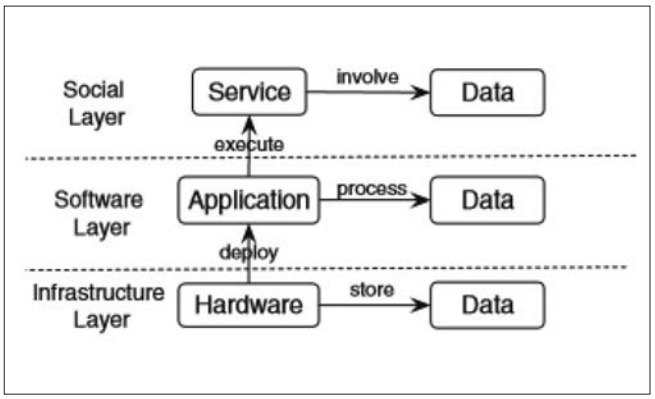
• Security property: مشخصه امنیت. در توسعهٔ این چارچوب منحصرا روی سه جنبه اصلی امنیت اطلاعات یعنی محرمانگی، یکپارچگی و دسترسی‌پذیری و زیرویژگی‌هایشان تمرکز شده است. شکل ۵ این ویژگی‌های امنیتی و زیرویژگی‌هایشان را نشان می‌دهد.

• asset: هرچیزی که برای سازمان ارزشمند است، مثل داده‌ها یا سرویس‌ها. شکل ۶ انواع دارایی‌هایی که در این چارچوب موردتوجه قرار گرفته‌اند و روابط میان آن‌ها را نشان می‌دهد. همان‌طور که مشاده می‌شود سرویس‌ها دارایی‌های لایه اجتماعی، برنامه‌های کاربردی که سرویس‌ها را اجرا می‌کنند دارایی‌های لایه نرم‌افزار، سخت‌افزاری که بستر استقرار برنامه‌های کاربردی است دارایی‌های لایه زیرساخت می‌باشند. علاوه بر این، داده‌ها دارایی هستند که در هر ۳ لایه وجود دارند.

• Interval: بازه زمانی یک هدف امنیتی. نشان‌دهندهٔ مدت زمانی



شکل ۵: سلسله مراتب ویژگی‌های امنیتی



شکل ۶ :. نمایی از دارایی‌ها

است که آن هدف اعمال می‌شود. هر تهدید می‌تواند یک عنصر زمان داشته باشد. این عنصر بیان می‌کند که آسیب در صورتی رخ خواهد داد که نقض قبل یا بعد از یک نقطه زمانی یا در طول یک بازه زمانی رخ داده باشد. بنابراین بُعد زمان روی تحلیل نیازمندی‌های امنیتی تاثیر دارد. از این رو در این چارچوب برای بازهٔ اجرای یک کار (Task) interval تعریف می‌شود. باید توجه داشت که یک goal هم می‌تواند برای نشان دادن interval استفاده شود. در این حالت منظور بازهٔ اجرای تمام کارهایی است که این هدف را عملیاتی می‌کنند. به این ترتیب اهداف امنیتی به‌طور ضمنی به نیازمندی‌های عملکردی سیستم مرتبط می‌شوند.

• importance: اهمیت یک هدف امنیتی نشان‌دهندهٔ اولویت آن هدف است. مقادیر ممکن برای این پارامتر {very low,low,medium,high,very high} می‌باشد.

• Security mechanism: سازوکار امنیتی روش عملیاتی کردن هدف امنیتی است. سازوکار امنیتی در این چارچوب به‌عنوان یک کار (task) ویژه تعریف می‌شود. رابطهٔ عملیاتی شدن میان سازوکارهای امنیتی و اهداف امنیتی یک رابطه چند به چند است، یعنی یک سازوکار امنیتی می‌تواند چندین هدف امنیتی را برآورده سازد و یک هدف امنیتی ممکن است به بیش از یک سازوکار امنیتی نیاز داشته باشد. لازم به توجه است که در این چارچوب مشخص نمی‌شود چه چیزی سازوکار است و چه چیزی نیست و در عوض سازوکارها از منابع مستقر شده، یعنی راه‌حل‌هایی که توسط الگوهای امنیتی موجود پیشنهاد شدند، گرفته می‌شوند. به این ترتیب سازوکارهای امنیتی خاص لایه، متناظر هستند با الگوهای امنیتی خاص لایه. به‌عنوان مثال ممیزی یک سازوکار امنیتی است که می‌تواند در لایه اجتماعی و برای تضمین یکپارچگی فعالیت‌های کسب‌وکار اعمال شود، در حالی که Input Guard یک سازوکار امنیتی خاص نرم‌افزار است که تمام ورودی های یک برنامه نرم‌افزاری را بررسی می‌کند. در این چارچوب سازوکارها در لایه‌های مختلف به‌کار گرفته می‌شوند و بخشی از مشخصات آن لایه محسوب می‌شوند.

۳- روش‌های تحلیل نیازمندی‌های امنیتی

شکل ۷ یک نمای کلی از فرآیند تحلیل را نشان می‌دهد. درون هر لایه اهداف امنیتی پالایش شده و شکل خاص آن تعریف می‌شود (هدف واقعی می‌شود) تا روش‌های ممکن عملیاتی شدن به شکل سازوکارهای امنیتی شناسایی شوند.

تحلیل‌های میان لایه‌ای، ملاحظات امنیتی را از یک لایه به یک لایه پایین‌تر منتشر می‌کنند. بعد از آن‌که تحلیل امنیت برای تمام لایه‌ها انجام شد، مجموعه‌ای از راه‌حل‌های امنیتی ارائه می‌شود.

کارهای تحلیلی که با نقشک چرخ دنده در شکل ۷ نشان داده شده‌اند کارهایی هستند که می‌توانند کاملا خودکار اجرا شوند (به کمک ابزار) و کارهایی که همراه با نقشک چرخ دنده نقشک انسان هم دارند کارهایی هستند که به‌صورت نیمه خودکار اجرا می‌شوند. مجموعه‌ای از قواعد استنتاج نیز برای پشتیبانی از تحلیل امنیت پیشنهاد شده‌اند که در Disjunctive Datalog پیاده‌سازی شده‌اند.

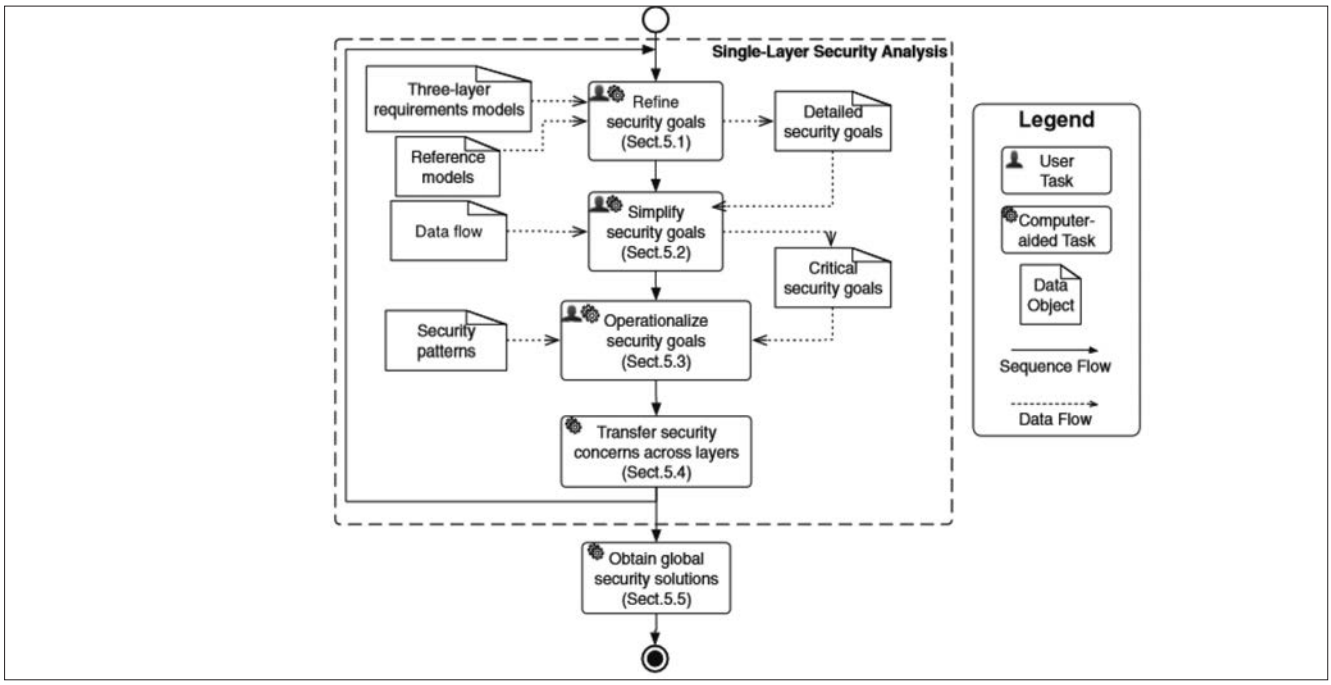
۳-۱-روش‌های پالایش

بعد از گرفتن نیازمندی‌های امنیتی اولیه سودبران به‌عنوان ورودی، تحلیل‌گران باید در یک چرخه تکرارشونده آن‌ها را پالایش کنند تا نیازهای واقعی سودبران به دست آمده و در نهایت بتوان آن نیازهای واقعی را عملیاتی کرد. این چارچوب سه روش پالایش پیشنهاد می‌دهد که در واقع مبتنی بر سه ویژگی اهداف امنیتی (یعنی ویژگی، دارایی و بازه زمانی) هستند. برای این که بتوان این روش‌ها را به‌صورت نیمه خودکار در ابزار پیشنهادی پیاده‌سازی کرد، آن‌ها را در قالب قواعد استنتاج نیز فرمال کرده‌اند. جدول ۱ این قواعد را نشان می‌دهد. مفهوم گزاره‌های استفاده شده در این قواعد در زیرآمده است:

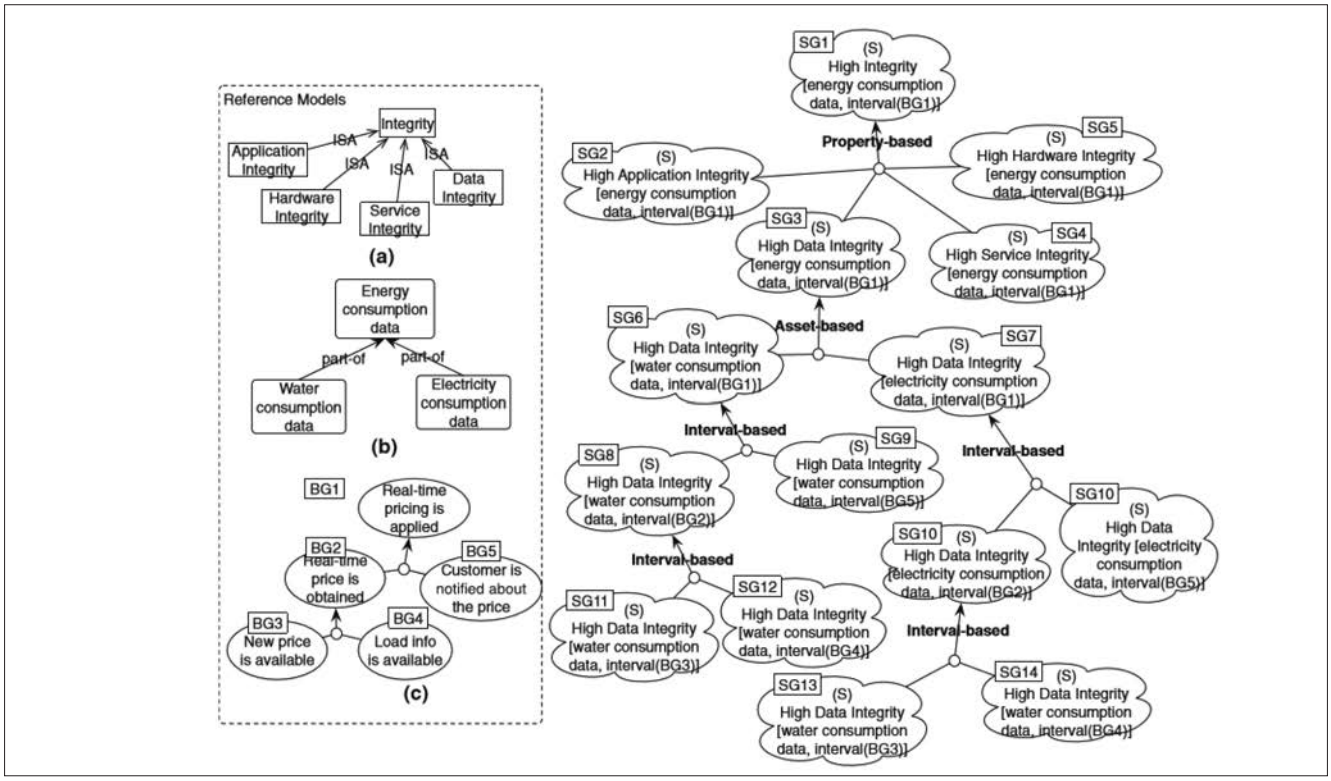
• گزاره has_attributes: چهار ویژگی یک هدف امنیتی یعنی، اهمیت (IMP)، ویژگی (SP)، دارایی (AS) و بازه زمانی (INT) را توصیف می‌کند.

• گزاره is_a: رابطهٔ خاص میان دو ویژگی امنیتی را نشان می‌دهد.

• گزاره part_of: رابطه بخشی میان دو دارایی را توصیف می‌کند.



شکل ۷: نمای کلی فرآیند سه لایه تحلیل نیازمندی های امنیتی



شکل ۸: پالایش‌های هدف امنیتی

گـزاره operationalize، refine، and_refine: روابط میان عناصر نیازمندی‌ها (اهداف G و کارها T) را نشان می‌دهد.

شـکل ۸ مثال هایی از پالایش اهداف امنیتی براسـاس هدف امنیتی High Integrity [energy consumption data, interval(BG1)] را نشان داده و هر سه روش پالایش را شامل می‌شود.

بخش سمت چپ شکل ۸ مدل‌های مرجعی را نشان می‌دهد که برای پالایش متناظر مورد اسـتفاده قرار گرفته‌اند. با اسـتفاده از این مثال هریک از این روش‌ها شرح داده می‌شود.

۳-۱-۱- پالایش مبتنی بر ویژگی امنیتی

پالایش امنیت از طریق ویژگی‌های امنیت به تحلیل‌گر کمک می‌کند

جدول ۱ : قواعد استنتاج برای روش‌های پالایش

No.	Content
REF.P	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, SP2, AS, INT) \wedge and\_refine(SG2, SG1)$ $\leftarrow is\_a(SP2, SP1) \wedge sg\_attributes(SG1, IMP, SP1, AS, INT)$
REF.A	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, SP, AS2, INT) \wedge and\_refine(SG2, SG1)$ $\leftarrow part\_of(AS2, AS1) \wedge sg\_attributes(SG1, IMP, SP, AS1, INT)$
REF.I.1	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, SP, AS, INT2) \wedge and\_refine(SG2, SG1)$ $\leftarrow interval\_of(INT1, G1) \wedge interval\_of(INT2, G2)$ $\wedge and\_refine(G2, G1) \wedge sg\_attributes(SG1, IMP, SP, AS, INT1)$
REF.I.2	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, SP, AS, INT2) \wedge refine(SG2, SG1)$ $\leftarrow interval\_of(INT1, G1) \wedge interval\_of(INT2, G2)$ $\wedge refine(G2, G1) \wedge sg\_attributes(SG1, IMP, SP, AS, INT1)$
REF.I.3	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, SP, AS, INT2) \wedge refine(SG2, SG1)$ $\leftarrow interval\_of(INT1, G) \wedge interval\_of(INT2, T)$ $\wedge operationalize(T, G) \wedge sg\_attributes(SG1, IMP, SP, AS, INT1)$

که تمام جنبه‌های ممکن امنیت را پوشش دهد.

معنای قاعده REF.P: اگر ویژگی امنیتی SP2 یک نوع ویژه از ویژگی امنیتی SP1 است (براساس سلسله مراتب ویژگی‌های امنیتی که در شکل ۵ نشان داده شد) آن گاه هدف امنیتی SG1 که مربوط به ویژگی امنیتی SP1 است به زیرهدف امنیتی SG2 که مربوط به SP2 می‌شود and_refine خواهد شد و سایر ویژگی‌های SG1 را به ارث می‌برد.

۳-۱-۲- پالایش مبتنی بر دارایی

پالایش اهداف امنیتی می‌تواند با پالایش دارایی‌ها و براساس روابط بخشی متناظر آن‌ها انجام شود.

قاعده REF.A: یک هدف امنیتی می‌تواند به زیراهداف امنیتی and-refine شود، هریک از این زیراهداف به بخشی از دارایی‌های هدف امنیتی اصلی مربوط می‌شوند و سایر ویژگی‌ها بدون تغییر باقی می مانند.

۳-۱-۳- پالایش مبتنی بر بازه زمانی

از آن جایی که یک بازه زمانی، دورهٔ زمانی معتبر بودن هدف امنیتی را تعیین می‌کند، تحلیل‌گر می‌تواند با پالایش یک بازه زمانی بلند مدت به بازه های زمانی کوتاه تر، قیود جزئی بیشتری را روی یک بازه زمانی خاص تعریف کند.

قاعده REF.I.1 و REF.I.2 : اگر بازه INT1 مربوط به هدف امنیتی SG1 بتواند به (and-)refine، INT2 شود، آن گاه می‌توان هدف امنیتی SG2 جدیدی به دست آورد که SG1 را از طریق بازه زمانی‌اش (and-)refine می‌کند.

قاعده REF.I.3: معنای مشابهی با دو قاعده بالا دارد اما روی ارتباط عملیاتی کردن متمرکز است.

۳-۱-۴- راهبردهای پالایش

فرآیندهای پالایش منعطف هستند، به این معنا که روش‌های پالایش مختلفی را می‌توان در هر دنباله‌ای و به هر میزانی به‌کار گرفت. در این چارچوب دو راهبرد برای پالایش اهداف امنیتی پیشنهاد شده است.

۱- راهبرد پالایش انتخابی: تحلیل‌گر با توجه به هدف امنیتی که قرار است پالایش شود و براساس تجربه، یک بُعد خاص برای پالایش تعیین می‌کند. بعد از انجام این پالایش، تحلیل‌گر باید اهداف امنیتی پالایش شده را با سودبران بررسی کند تا مشخص شود که به تمام آن‌ها نیاز است یا خیر. اگر یک هدف امنیتی موردنیاز سودبران نباشد تحلیل‌گر باید آن را از پالایش‌های بعدی حذف نماید. به این ترتیب تحلیل‌گر قادر خواهد بود نیازهای امنیتی دقیق سودبران را به دست آورد که به‌صورت معمول و در حین مراحل اولیه تحلیل امنیت به سادگی قابل بیان نبودند. هرس کردن اهداف غیرلازم فضای پالایش را کاهش می‌دهد. شکل ۸ نمونه ای از پالایش با این راهبرد است.

۲- راهبرد پالایش جامع: در این روش تمام پالایش‌های ممکن برای یک هدف امنیتی پیدا می‌شوند. در این حالت هیچ بُعد پالایش توسط کاربر هرس نمی‌شود. این راهبرد به کامل بودن تحلیل کمک می‌کند اما می‌تواند تعداد زیادی هدف امنیتی اضافه نیز به همراه داشته و تحلیل‌های بعدی را پیچیده سازد.

براساس مزایا و معایب این دو راهبرد پیشنهاد می‌شود که از راهبرد ترکیبی برای پالایش اهداف امنیتی استفاده شود. تحلیل‌گران باید ابتدا با استفاده از راهبرد انتخابی نیازهای دقیق سودبران را استخراج نمایند. سپس براساس این نیازهای امنیتی دقیق تحلیل‌گران می‌توانند برای کاوش فضای پالایش نیازهای امنیتی از راهبرد پالایش جامع استفاده کنند.

۳-۲- روش‌های ساده‌سازی

بعد از این که اهداف امنیتی به اهداف دقیق‌تر پالایش شد، چه به روش انتخابی و چه به روش جامع، لازم است فضای اهداف امنیتی با استفاده از روش‌های ساده‌سازی هرس شود. باید توجه داشت که، تحلیل هرس اشاره شده در تحلیل پالایش به این موضوع می‌پردازد که آیا یک هدف امنیتی مطلوب سودبران است یا خیر اما در روش‌های ساده‌سازی، تمرکز روی تحلیل بحرانی بودن اهداف امنیتی موردنظر

جدول ۲: قواعد استنتاج برای تحلیل کاربردپذیری

No.	Content
APP.1	$is\_applicable(SG) \leftarrow (sg\_attributes(SG, \_, data\_confidentiality, AS, INT) \vee sg\_attributes(SG, \_, data\_integrity, AS, INT) \vee sg\_attributes(SG, \_, data\_availability, AS, INT)) \wedge interval\_of(INT, T) \wedge data(AS) \wedge (has\_input(T, AS) \vee has\_output(T, AS))$
APP.2	$is\_applicable(SG) \leftarrow service(AS) \wedge (sg\_attributes(SG, \_, service\_integrity, AS, \_) \vee sg\_attributes(SG, \_, service\_availability, AS, \_))$
APP.3	$is\_applicable(SG) \leftarrow application(AS) \wedge (sg\_attributes(SG, \_, application\_integrity, AS, \_) \vee sg\_attributes(SG, \_, application\_availability, AS, \_))$
APP.4	$is\_applicable(SG) \leftarrow hardware(AS) \wedge (sg\_attributes(SG, \_, hardware\_integrity, AS, \_) \vee sg\_attributes(SG, \_, hardware\_availability, AS, \_))$

جدول ۳: قواعد استنتاج تحلیل تهدید

No.	Content
$TH.1$	$threaten(TH, SG) \leftarrow sg\_attributes(SG, \_, SP, AS, INT) \wedge is\_a(SP, confidentiality) \wedge th\_attributes(TH, information\_disclosure, AS, INT)$
$TH.2$	$threaten(TH, SG) \leftarrow sg\_attributes(SG, \_, SP, AS, INT) \wedge is\_a(SP, integrity) \wedge th\_attributes(TH, tampering, AS, INT)$
$TH.3$	$threaten(TH, SG) \leftarrow sg\_attributes(SG, \_, SP, AS, INT) \wedge is\_a(SP, availability) \wedge th\_attributes(TH, denial\_of\_service, AS, INT)$

(اهداف مطلوب سودبران) است. دو روش ساده‌سازی در این چارچوب ارائه می‌شود:

۳-۲-۱ تحلیل کاربردپذیری

وقتی گفته می‌شود یک هدف امنیتی کاربردپذیر است یعنی با توجه به معنای ویژگی‌هایش (ویژگی، دارایی و ...) محسوس است در غیر این صورت گفته می‌شود کاربردپذیر نیست.

برای تعیین کاربردپذیری اهداف امنیتی، ابتدا باید مشخص شود که ویژگی امنیتی برای نوع دارایی کاربردپذیر است یا خیر. به‌عنوان مثال، ویژگی امنیتی «یکپارچگی سخت‌افزار» تنها با دارایی سخت‌افزار موردتوجه قرار می‌گیرد. اگر یک هدف امنیتی تلاش می‌کند که از یکپارچگی سخت‌افزار برای دارایی داده محافظت کند به آن کاربردناپذیر گفته می‌شود. سپس باید ویژگی امنیت در ارتباط با داده (مثلا یکپارچگی داده) بررسی شود؛ یعنی بررسی شود که آیا داده در طول بازه زمانی هدف وجود دارد یا خیر. به‌عنوان مثال اگر یک هدف امنیتی به یکپارچگی دارایی داده در طول یک بازه زمانی مشخص می‌پردازد اما داده در آن بازه زمانی واقعا درگیر نمی‌شود، آن هدف امنیتی کاربردناپذیر است. برای انجام این تحلیل، از اطلاعات جریان دادهٔ هر کار، یعنی ورودی و خروجی هر کار، استفاده می‌شود.

برای تسهیل تحلیل کاربردپذیری ۴ قاعده نیز معرفی می‌شود که در جدول ۲ نشان داده شده‌اند. براساس این قواعد، هدف امنیتی High Data Integrity [water consumption data, new price is available (BG3)] کاربردناپذیر است زیرا دارایی «داده مصرف آب» در بازه زمانی اجرای BG3 درگیر نمی‌شود.

۳-۲-۲- تحلیل تهدید

برای هر هدف امنیتی باید تهدیداتی که برآورده کردن آن هدف را مختل می‌سازند نیز شناسایی شوند. این کار به تشخیص بحرانی بودن هدف کمک می‌کند. برای انجام این تحلیل دو راه وجود دارد:

۱- استفاده از روش‌های موجود تحلیل تهدید ۲- در صورت وجود استفاده از گزارش های مرتبط با تهدیدات سیستم هدف.

هر تهدید شناسایی شده با نام، نوع، دارایی تهدید شده، زمان تهدید مشخص می‌شود و براین اساس می‌توان مشخص کرد کدام اهداف امنیتی مورد هدف این تهدید قرار می‌گیرند.

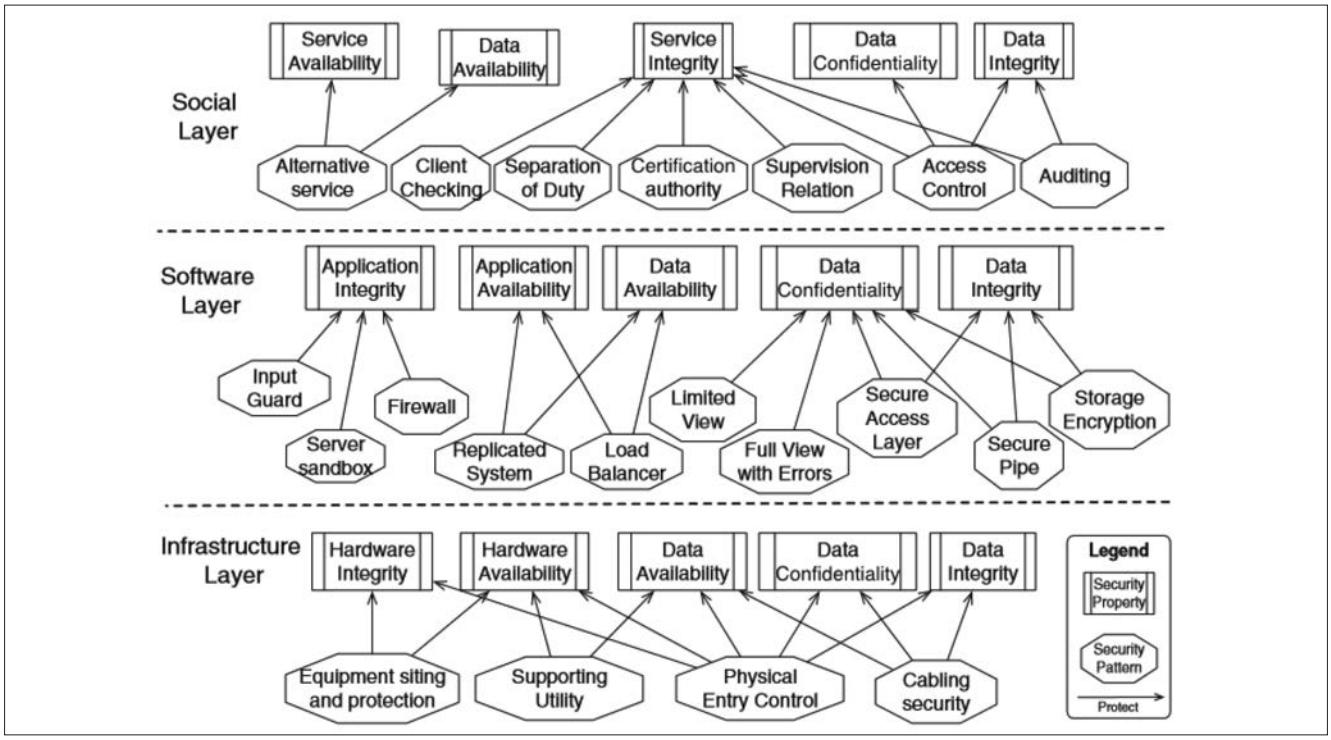
نوع تهدید با استفاده از دسته‌بندی STRIDE مشخص می‌شود. هر دسته‌بندی به یک نوع خاص از ویژگی امنیتی مربوط می‌شود، مثلا نوع تهدید Tampering به ویژگی امنیت Integrity نگاشت می‌شود. مجموعه‌ای از قواعد تحلیل تهدید در قالب TH1-3 در جدول ۳ ارائه شده است.

۳-۲-۳- تحلیل بحرانی بودن

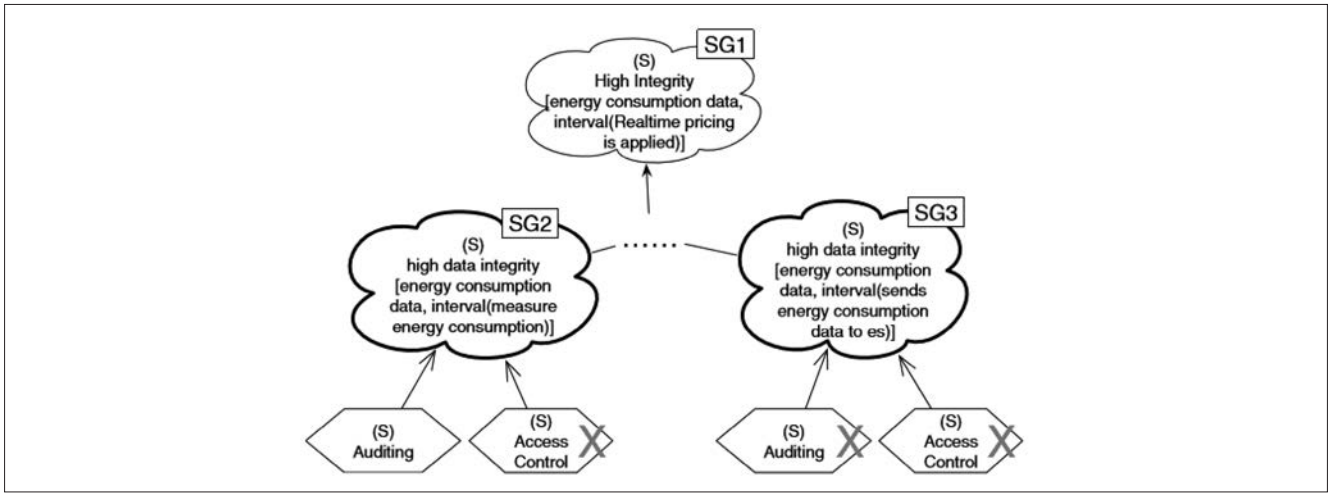
براساس تحلیل کاربردپذیری و تحلیل تهدید مشخص می‌شود که یک هدف امنیتی بحرانی است یا خیر:

۱- اگر یک هدف امنتیتی کاربردپذیر بوده و هدف تهدیدات خاصی باشد یک هدف امنیتی بحرانی محسوب می‌شود.

۲- اگر یک هدف امنیتی کاربردپذیر باشد اما به هیچ تهدیدی مرتبط



شکل ۹: فهرست الگوهای امنیتی استفاده شده در سه لایه



شکل ۱۰: مثالی از عملیاتی کردن اهداف امنیتی بحرانی

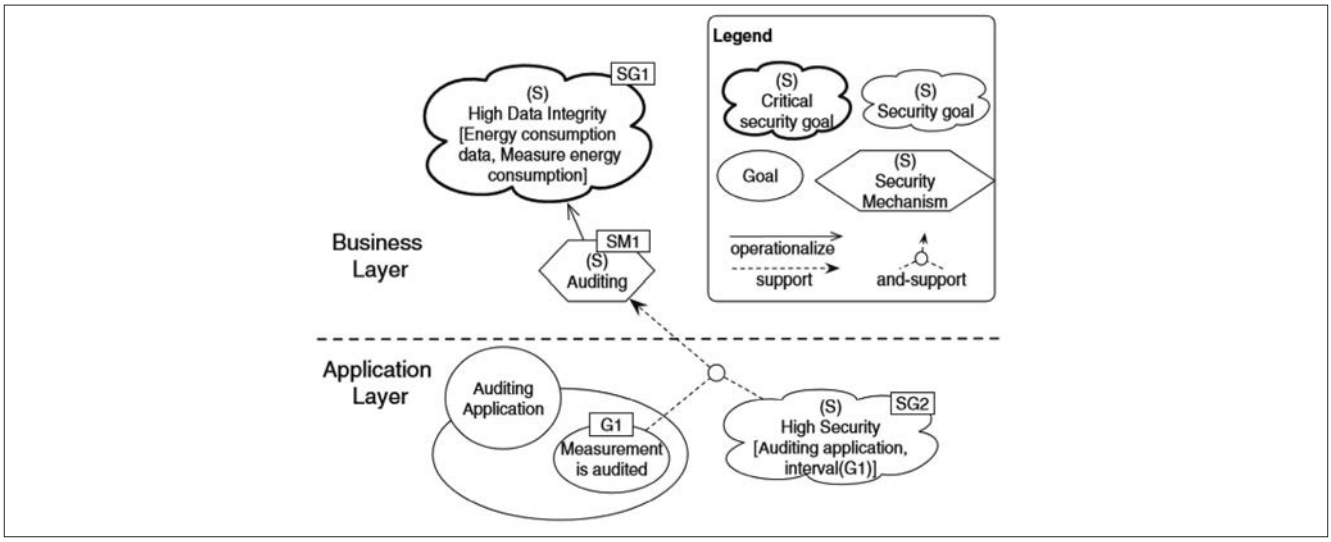
نشـود تحلیل‌گر باید به‌صورت دسـتی بحرانی بودن آن هدف امنیتی را مشـخص کند. اگر تحلیل‌گر دانش امنیتی کافی نداشته باشد یک راه‌حل محافظه‌کارانه این اسـت که تمام اهـداف امنیتی کاربردپذیر بحرانی قلمداد شوند. این روش کامل بودن تحلیل را تضمین می‌کند اما پیچیدگی تحلیل بعدی را افزایش می‌دهد.

۳-۲-۴- ترکیب ساده‌سازی و پالایش

تحلیل ساده‌سازی به دو روش قابل اعمال است.

اول، تحلیل‌گـران می‌توانند تحلیل ساده‌سـازی را همـراه با پالایش انتخابـی هدف امنیتـی انجام دهند، این مشـخص می‌کنـد که آیا هدف امنیتی به پالایش بیشـتر نیـاز دارد یا خیر. برای مثال اگر یک هدف امنیتی پالایش شـده کاربردپذیر نباشـد از پالایش‌های بعدی حذف می‌شـود، همچنین اگر یک هدف امنیتی پالایش شده بحرانی تشـخیص داده شـود نیاز به پالایش بیشـتر نخواهد داشـت و برای عملیاتی شـدن در گام بعدی تحلیل مورد بررسی قرار خواهد گرفت. برای هدف امنیتی پالایش شـده‌ای که کاربردپذیـر بوده اما بحرانی نیسـت، تحلیل‌گر می‌تواند به پالایش آن ادامه داده و بیشـتر ارزیابی کند. اگر این هدف قابل پالایش بیشـتر نباشد تحلیل‌گر باید بحرانی بودن آن را به‌صورت دستی مشخص کند.

دوم، تحلیل‌گر می‌تواند ساده‌سـازی را روی تمام اهداف امنیتی که به روش جامع پالایش شـده‌اند اجرا کند. اگرچه این تحلیل به شناسایی



شکل ۱۱: تحلیل میان لایه‌ای سازوکارهای امنیتی

سریع اهداف امنیتی بحرانی کمک می‌کند اما لازم است که تحلیل‌گر بحرانی بودن سایر اهداف امنیتی کاربردپذیر را به‌صورت دستی ارزیابی کند که کار ساده ای نیست.

۳-۳- روش‌های عملیاتی کردن

روش‌های عملیاتی کردن، سازوکارهای امنیتی موردنیاز برای تحقق یک هدف امنیتی بحرانی را تولید می‌کنند. به این منظور از الگوهای امنیتی استفاده می‌شود تا برای عملیاتی کردن اهداف امنیتی دانش امنیتی زیادی موردنیاز نباشد.

الگوهای امنیتی برای مسائل امنیتی شناخته شده در یک زمینهٔ خاص، راه‌حل‌های امنیتی قابل اثباتی ارائه می‌دهند. شکل ۹ فهرست الگوهای امنیتی استفاده شده در سه لایه و نیز ویژگی‌های امنیتی به دست آمده از آن الگوها را نشان می‌دهد. همان‌طور که در این شکل مشخص است، یک الگو می‌تواند روی چندین هدف امنیتی قابل اعمال باشد و یک هدف امنیتی می‌تواند چندین الگوی امنیتی داشته باشد.

در مجموع از ۲۱ الگوی امنیتی استفاده شده است، ۷ الگو در لایه اجتماعی، ۱۰ الگو در لایه نرم‌افزار و ۴ الگو در لایه زیرساخت.

برای عملیاتی کردن یک هدف امنیتی، ابتدا براساس ویژگی امنیتی الگو تمام الگوهای امنیتی نامزد شناسایی می‌شوند. به‌عنوان مثال همان‌طور که در شکل ۱۰ نشان داده شده است دو هدف امنیتی بحرانی SG2 و SG3 ویژگی امنیتی یکپارچگی داده را مورد توجه قرار می‌دهند که براین اساس دو الگوی امنیتی نامزد برای هریک از این اهداف امنیتی شناسایی می‌شود. بعد از شناسایی الگوهای امنیتی نامزد تحلیل‌گر باید به‌صورت دستی کاربردپذیری این الگوها را بررسی کند. به‌طور مشخص تر، تحلیل‌گر باید سیستم هدف و محیط را در برابر زمینه و نیروهای الگوهای نامزد بررسی کند و سپس تصمیم بگیرد که کدام الگو اعمال شود. در شکل ۱۰ الگوهای کاربردناپذیر با علامت ضربدر مشخص شده‌اند.

اگر یک هدف امنیتی در یک لایه و با استفاده از الگوهای امنیتی خاص آن لایه قابل عملیاتی شدن نباشد دو دلیل می‌تواند داشته باشد:

۱- تهدیدات بالقوهٔ آن هدف امنیتی در لایه فعلی وجود ندارند و از این رو لازم است این هدف امنیتی در لایه‌های پایین‌تر بیشتر تحلیل و تشریح شود.

۲- فهرست الگوهای امنیتی برای برآورده ساختن این هدف مناسب نیستند و نیاز به گسترش فهرست می‌باشد.

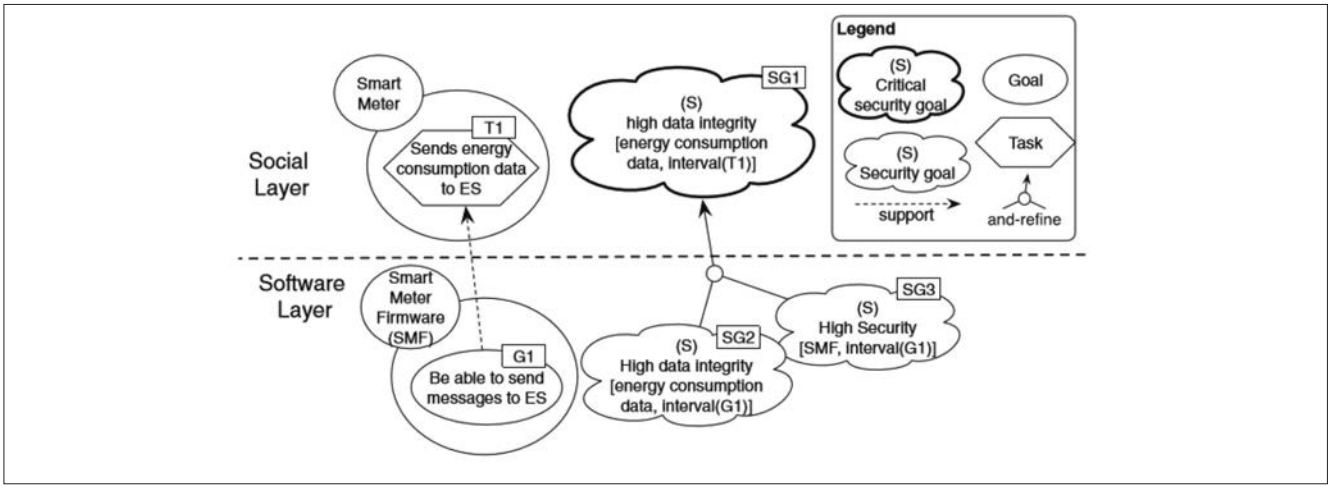
۳-۴- روش‌های تحلیل میان لایه‌ای

بعد از تمام شدن تحلیل امنیتی در یک لایه، نوبت به تحلیل امنیتی لایه بعد می‌رسد، یعنی تولید مجموعه‌ای از اهداف امنیتی در لایه بعد براساس نتایج تحلیل این لایه. سپس یک دور تحلیل امنیتی جدید برای لایه بعد و با استفاده از اطلاعات موجود در آن لایه انجام خواهد گرفت.

تحلیل میان لایه‌ای روی تحلیل تاثیرات سازوکارهای امنیتی اعمال شده و اهداف امنیتی بحرانی در یک لایه تمرکز دارد.

۳-۴-۱- تاثیرات سازوکار امنیتی اعمال شده

بعد از عملیاتی شدن یک سازوکار امنیتی خاص در یک لایه، تحلیل‌گر ابتدا باید بررسی کند که آیا این سازوکار امنیتی براساس مشخصات خود نیازمند پشتیبانی آرتیفکت های لایه پایین‌تر است یا خیر. اگر این طور باشد سازوکار امنیتی به‌عنوان یک کار خاص، معرفی‌کنندهٔ نیازمندی عملکردی به یک لایه پایین‌تر خواهد بود. همان‌طور که در شکل ۱۱ مشاهده می‌شود، تعیین شده است که سازوکار Auditing با برنامه Auditing در لایه نرم‌افزار پیاده‌سازی شود. بنابراین یک هدف نرم‌افزاری جدید به اسم Measurement is audited (G1) برای برنامه کاربردی معرفی می‌شود.



شکل ۱۲: تحلیل امنیت میان لایه‌ای برای اهداف امنیتی

جدول ۴: قواعد استنتاج تحلیل میان لایه‌ای

No.	Content
CRO.1	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, security, A, INT)$
	$\wedge support(SG2, SM) \leftarrow operationalize(SM, SG1) \wedge sg\_importance(SG1, IMP)$
	$\wedge support(G, SM) \wedge has(A, G) \wedge interval\_of(INT, G)$
CRO.2	$\#create(sec\_goal(SG2)) \wedge sg\_attributes(SG2, IMP, SP, AS, INT2)$
	$\wedge \#create(sec\_goal(SG3)) \wedge sg\_attributes(SG3, IMP, security, A, INT2)$
	$\wedge and\_refine(SG2, SG1) \wedge and\_refine(SG3, SG1) \leftarrow interval\_of(INT1, T)$
	$\wedge sg\_attributes(SG1, IMP, SP, AS, INT1) \wedge support(G, T)$
	$\wedge has(A, G) \wedge interval\_of(INT2, G)$

تفاوت سازوکار امنیتی با یک کار عام این است که سازوکار برای برآورده شدن هم به پشتیبانی عملکردی و هم به پشتیبانی امنیتی یک لایه پایین‌تر از خود نیاز دارد. در غیر این صورت در اجرای سازوکار اختلال روی داده و در محافظت از سیستم با شکست مواجه می‌شود. همان‌طور که شکل ۱۲ نشان می‌دهد SG2 برای تضمین امنیت برنامه کاربردی Auditing به لایه نرم‌افزار معرفی می‌شود. بنابراین SG2 همراه با G1 از سازوکار امنیتی SM1 در لایه اجتماعی پشتیبانی می‌کنند.

جدول ۴ قواعد استنتاج تحلیل میان لایه‌ای را نشان می‌دهد.

تحلیل فوق باید برای تمام سازوکارهای امنیتی که اهداف امنیتی را عملیاتی می‌سازند اجرا شود. اگر هدف امنیتی با چندین سازوکار امنیتی عملیاتی می‌شود تمام آن سازوکارها باید بررسی شوند.

۳-۴-۲- تاثیرات اهداف امنیتی بحرانی

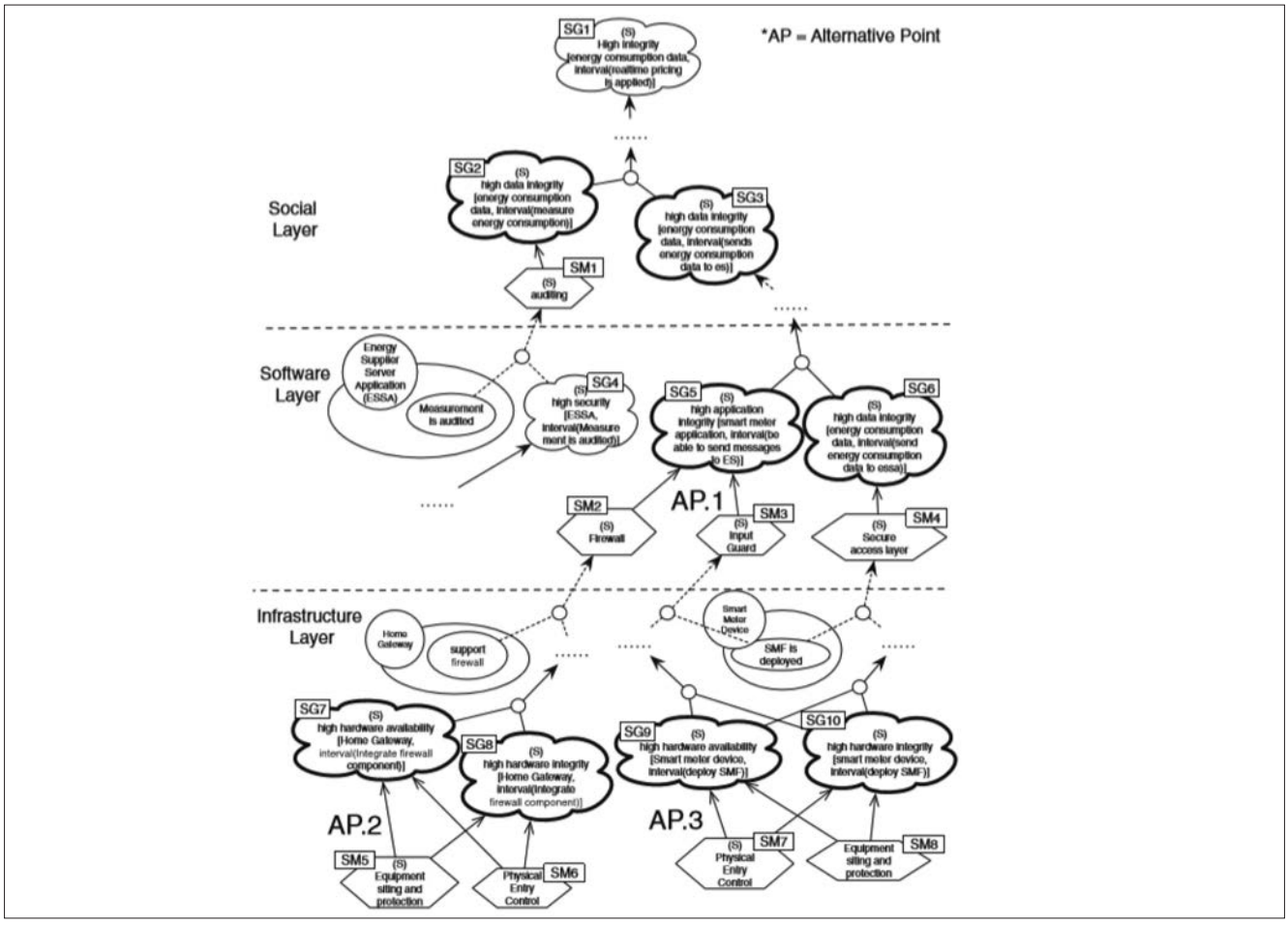
برای هر هدف امنیتی بحرانی که در یک لایه شناسایی شده است، باید بررسی می‌شود که آیا این هدف موضوعات امنیتی لایه پایین‌تر را نیز در بر می‌گیرد یا خیر. ابتدا تهدیدات خاص لایه برای دارایی اصلی لایه بعد تحلیل می‌شوند؛ سپس امنیت آرتیفکت‌های پشتیبانی کننده در لایه بعد مورد توجه قرار می‌گیرند، چرا که حمله کنندگان می‌توانند به‌صورت غیرمستقیم و با استخراج آسیب‌پذیری‌های آرتیفکت‌های پشتیبانی‌کننده،دارایی اصلی را مختل کنند. (شکل ۱۲)

بعد از این که این تحلیل میان لایه‌ای برای یک لایه انجام شد، تا رسیدن به لایه آخر تحلیل به‌صورت تکرارشونده برای لایه بعدی انجام خواهد شد.

۳-۵- به دست آوردن راه‌حل‌های امنیتی سراسری

با انجام تحلیل رو به عقب روی مدل هدف، یعنی جستجوی راه‌حل‌ها از اهداف ریشه به سمت اهداف برگ، مجموعه‌ای از راه‌حل‌های امنیتی جامع تولید می‌شوند. هر راه‌حل شامل تعدادی سازوکار امنیتی است که از لایه اجتماعی تا لایه زیرساخت متغیر هستند.

نمونه ای از مدل جامع هدف امنیتی در شکل ۱۳ نشان داده شده است. هر نقطه جایگزین (AP) در این شکل بیانگر این است که سازوکارهای امنیتی جایگزینی وجود دارند که می‌توانند برای برآورده کردن هدف امنیتی به‌کار گرفته شوند. باید توجه داشت که انتخاب یک سازوکار امنیتی به جای یک سازوکار دیگر (مثلا SM2 به جای SM3 در AP1) منجر به تاثیرات مختلفی روی تحلیل امنیتی لایه زیرساخت شده و در نتیجه راه‌حل های جامع متفاوتی را تولید می‌کند.



شکل ۱۳: بخشی از یک مدل هدف امنیتی جامع

۴- اعتبارسنجی

بـا اعمال کردن این چارچوب روی سـناریوی قیمت‌دهی بیدرنگ در شـبکه هوشـمند می‌توان عملکرد آن را ارزیابی کرد. در این ارزیابی هدف امنیتی «محرمانگی اطلاعات صورت حسـاب مشتری» تحلیل می‌شود.

در واقع این ارزیابی به دنبال پاسخ برای سوالات زیر است:

RQ1: آیـا این رویکـرد برای STS های مقیاس بزرگ قابل اسـتفاده است؟

- RQ1.1: آیا می‌توان به روشـی موثر مدل‌های نیازمندی سه لایه را برای STS مقیاس بزرگ ساخت؟

□RQ1.1.1 : آیا جمع‌آوری اطلاعات دامنه برای سـاخت این مدل‌ها آسان است؟

- RQ1.1.2: برای ساخت این مدل‌ها به چه میزان کار نیاز است؟
- RQ1.2 : آیـا می‌توان تحلیل امنیتـی جامع را به‌صورت موثر روی STSهای مقیاس بزرگ انجام داد؟

□RQ1.2.1: آیا به تخصص/دانش امنیتی بیشتری نیاز است یا خیر؟

- RQ1.2.2: آیا در اعمال روش‌های تحلیل دشواری وجود دارد؟
- RQ1.2.3: برای انجام تحلیل امنیت به چه میزان کار نیاز است؟

□ RQ2: تا چه اندازه این روش در محافظت امنیتی جامع نقش دارد؟

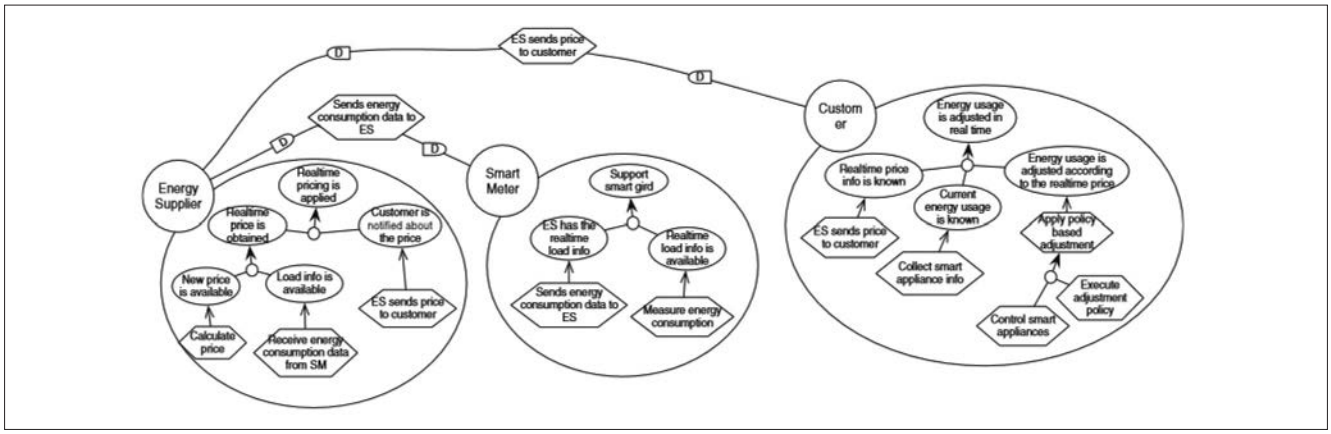
- RQ2.1: آیا می‌توان راه‌حل‌های امنیتی جامع شناسایی کرد؟
- RQ2.2: چه تعداد جایگزین امنیتی شناسایی می‌شود؟
- RQ2.3: کدام یک از عامل‌ها روی نتایج تحلیل امنیتی تاثیر دارند؟

۴-۱- ساخت مدل نیازمندی سه لایه

برای ساخت این مدل ابتدا از لایه اجتماعی شروع می‌شود:

- در اولیـن لایه تمرکز منحصرا روی جنبه‌هـای تجاری و اجتماعی فرانامه (سناریو) قرار دارد و از مسائل فنی صرف نظر می‌شود.
- هنـگام تهیه مدل نیازمندی داخل هر عامل، به تعریف عملیاتی هر کار (task) در لایه اجتماعی توجه می‌شـود یعنی هر کار یک فعالیت از فرآیند کسب‌وکار است.
- از روش بالا به پایین استفاده می‌شود، یعنی ابتدا هر فعالیت فرآیند کسـب‌وکار به‌عنوان یک کار در لایه اجتماعی مدل‌سـازی می‌شـود سپس با پرسیدن سـوالات «چرا» اهداف به دست آمده از این کارها شناسایی می‌شوند.

شکل ۱۴ مدل نیازمندی لایهٔ اجتماعی را نشان می‌دهد.



شکل ۱۴: مدل نیازمندی لایه اجتماعی در فرانامهٔ شبکه هوشمند

- (ساخت لایه نرم‌افزار) بعد از ساختن مدل نیازمندی در لایه اجتماعی، پیوندهای پشتیبانی میان لایه اجتماعی و لایه کاربردی مطلوب (لایه کاربردی که قرار است ایجاد شود) تحلیل می‌شود. بررسی می‌شود که آیا هر کاربرگ به‌طور کامل توسط افراد انجام می‌شود یا خیر. اگر پاسخ این سوال منفی باشد برنامه‌های نرم‌افزاری درگیردر این فعالیت شناسایی شده و براساس آن ها عناصر لایه کاربرد، شامل پیوندهای پشتیبانی که دو لایه را به هم مرتبط می‌سازند، مدل‌سازی می‌شوند. با تحلیل کردن پیوندهای پشتیبانی میان لایه‌ها، فهرستی از عامل‌های کاربرد به دست می‌آید که هریک از آن‌ها یک یا چند هدف نیازمندی دارند.

- براساس این مدل‌ها، نیازمندی‌های هر عامل در لایه نرم‌افزار تشریح می‌شود تا توابع برنامه‌های کاربردی (یعنی تعریف عملیاتی کارهای نرم‌افزار) به دست بیاید.

- اگر مدل‌های معماری نرم‌افزار وجود داشته باشند که بتوان از آنها به‌عنوان ورودی استفاده کرد، ساخت مدل نیازمندی در این لایه می‌تواند به شیوه پایین به بالا نیز انجام شود.

- (ساخت لایه زیرساخت) بعد از پایان یافتن مدل‌سازی نیازمندی‌ها در لایه نرم‌افزار، مدل نیازمندی لایه زیرساخت نیز به همین شیوه ایجاد می‌شود.

- در نهایت مدل سه لایه نیازمندی‌ها برای این سناریو حاصل می‌شود. (شکل ۱۵)

۴-۱-۱- ارزیابی

ساخت این مدل سه گام اصلی داشت:

گام اول : جمع‌آوری اطلاعات موردنیاز سه لایه

گام دوم: رفع تناقضات از اطلاعات به دست آمده از منابع گوناگون (یک دست‌سازی اطلاعات منابع مختلف)

پاسخ سوال RQ1.1.1: جمع‌آوری اطلاعات مرتبط با دامنه آسان نبود به خاطر روشی که در جمع‌آوری داده استفاده شد و با تغییر آن می‌توان این فرایند را تسهیل کرد.

گام سوم: ساخت مدل سه لایه (شکل ۱۵) (پاسخ به سوال RQ1.1.2)

با توجه به ابزار و جداسازی مفهومی لایه‌ها تحلیل‌گر می‌تواند بر پیچیدگی STS ها فائق آید و مدل سه لایه نیازمندی‌ها را بسازد (پاسخ سوال RQ1.1)

۴-۲- تحلیل نیازمندی‌های امنیتی در سه لایه

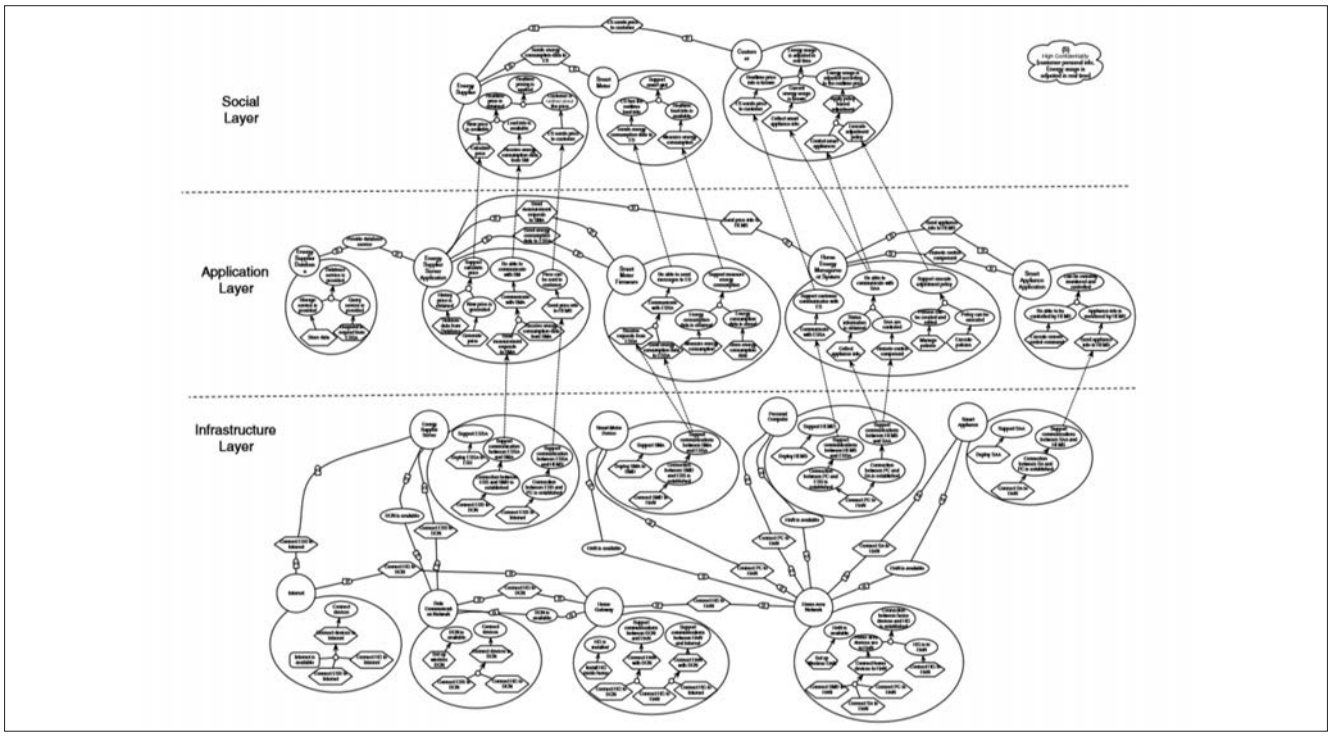
با داشتن مدل نیازمندی سه لایه فوق به‌عنوان ورودی، روش ذکر شده در بخش‌های قبلی گام به گام اعمال می‌شوند تا مدل جامع هدف امنیتی تولید شود. کار از هدف امنیتی ریشه شروع می‌شود:

۱- نیازهای امنیتی سطح بالای سودبران تحلیل می‌شود.

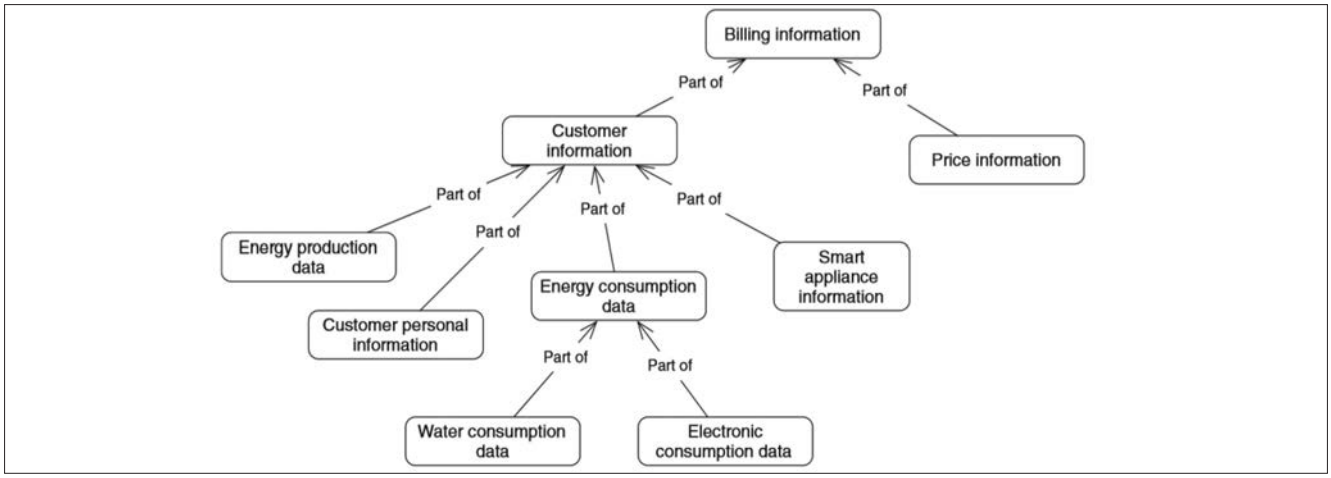
۲- هدف امنیتی سطح بالا پالایش می‌شود تا جایی که بتوان اهداف امنیتی بحرانی را شناسایی کرد. به این منظور از یک روش ترکیبی با یک ترتیب نوآورانه استفاده شد، یعنی ابتدا مدل امنیتی اولیه از طریق ویژگی‌های امنیتی (طبقه‌بندی ارائه شده در شکل ۵) پالایش می‌شود، سپس از طریق دارایی‌ها (شکل ۱۶) و در نهایت از طریق بازه زمانی (شکل ۱۵). بعد از هر پالایش، با پرسیدن این سوال نتایج ارزیابی می‌شوند: «آیا تمام اهداف امنیتی به دست آمده موردنیاز سودبران هستند؟» سپس اگر یک هدف امنیتی پالایش شده موردنیاز سودبران نباشد از تحلیل بعدی حذف می‌شود (شکل ۱۵ قسمت بالا). لازم به ذکر است که تعامل مستقیم با سودبران موردنیاز نیست (در این فرانامه استفاده نشده است) و براساس دانش جمع‌آوری شده، نسبت به این که اهداف امنیتی موردنیاز سودبران هستند یا خیر تصمیم‌گیری می‌شود.

۳- انجام تحلیل پالایش جامع روی هدف امنیتی که منعکس کننده نیازهای امنیتی سودبران است و کاوش تمام پالایش‌های ممکن آن هدف.

۴- انجام تحلیل ساده‌سازی روی تمام اهداف امنیتی که با پالایش جامع حاصل شدند، این تحلیل نیازمند دانش در خصوص تهدیدات سیستم مورد مطالعه است (اینجا شبکه هوشمند) که به این منظور و در این سناریو از گزارش های موجود استفاده شده است. شکل ۱۷ قسمت پایین حاصل فرآیند ساده‌سازی را نشان می‌دهد.



شکل ۱۵: مدل سه لایهٔ نیازمندی‌ها برای شبکه هوشمند



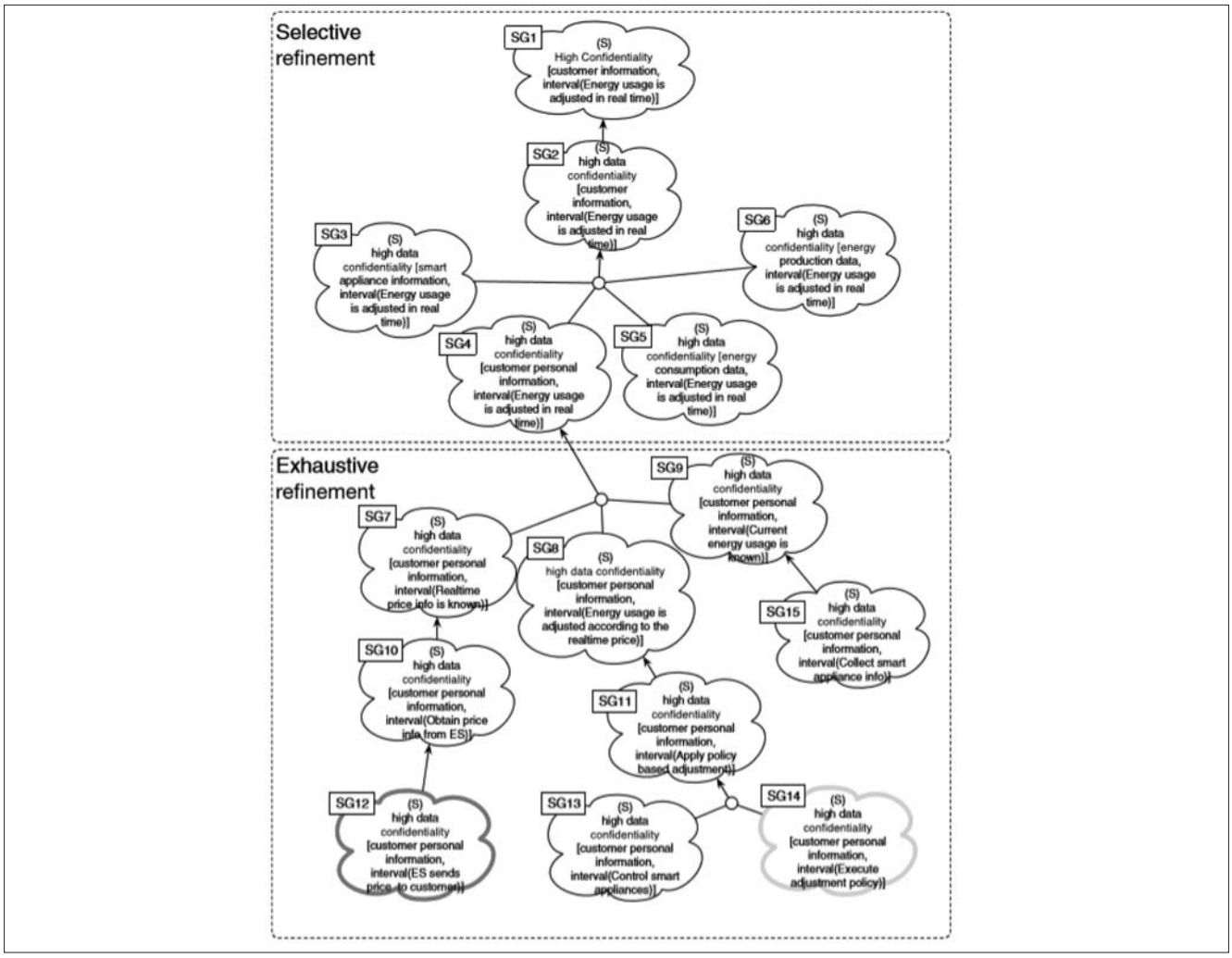
شکل ۱۶: منابع مورداستفاده در فرانامه مورد بررسی

۵- عملیاتی کردن هدف امنیتی: بعد از تعیین اهداف امنیتی بحرانی، تحلیل عملیاتی کردن براساس الگوی امنیتی انجام می‌شود تا این اهداف شناسایی شده عملیاتی شوند. ابتدا برای هر هدف امنیتی بحرانی فهرستی از الگوهای امنیتی نامزد (به‌صورت خودکار یا ابزار) تولید می‌شود، سپس زمینهٔ هر نامزد از لحاظ کاربردپذیری بررسی می‌شود (به‌صورت دستی). به‌عنوان مثال زمینهٔ کنترل دسترسی (به‌عنوان سازوکار امنیتی شناسایی شده) به‌صورت دستی بررسی می‌شود، یعنی «هر محیطی که در آن منابعی وجود دارد و دارایی‌های آن منابع نیاز به کنترل شدن دارند».

این زمینه‌ها را می‌توان براساس ویژگی‌های اهداف امنیتی (یعنی دارایی و ویژگی امنیتی) استنتاج نمود.

۶- تحلیل میان لایه‌ای: بعد از اتمام تحلیل عملیاتی کردن در یک لایه، با استفاده از پیوندهای میان لایه‌ای تحلیل میان لایه‌ای انجام می‌شود. پیوندهای میان لایه‌ای که در مدل سه لایهٔ هدف عملکردی مدل‌سازی می‌شوند، ملاحظات امنیتی را به لایه‌های پایین‌تر منتقل نموده و مولفه‌های سیستمی متناظر در آن لایه را مورد هدف قرار می‌دهد.

۷- تحلیل جامع راه‌حل امنیتی: با تکرار تحلیل امنیت در هریک از سه لایه، تحلیل امنیتی با رسیدن به یک مدل جامع هدف امنیتی



شکل ۱۷: پالایش اهداف امنیتی در لایه اجتماعی

به پایان می‌رسد (شکل ۱۸). تحلیل اقناع رو به عقب روی این مدل انجام می‌شود تا تمام راه‌حل‌های جامع امنیتی ممکن برای کل سیستم شناسایی شوند. هر کدام از این راه‌حل‌ها شامل راه‌حل‌های خاصی برای لایه‌های مختلف هستند و مولفه‌های مختلف سیستم را پوشش می‌دهند. به‌عنوان مثال راه‌حل امنیتی زیر از ۱۰ سازوکار امنیتی تشکیل شده است (هر سازوکار راه‌حلی است که یک الگوی امنیتی معرفی می‌کند)، در واقع دارای یک سازوکار در لایه اجتماعی، ۴ سازوکار در لایه نرم‌افزار و ۵ سازوکار در لایه زیرساخت می باشد. باید توجه داشت که برآورده کردن هدف امنیتی ریشه نیازمند این است که تمام این ۱۰ سازوکار امنیتی پیاده‌سازی شوند که ممکن است بسیار پرهزینه باشد:

راه‌حل ۱ (۱۰ سازوکار):

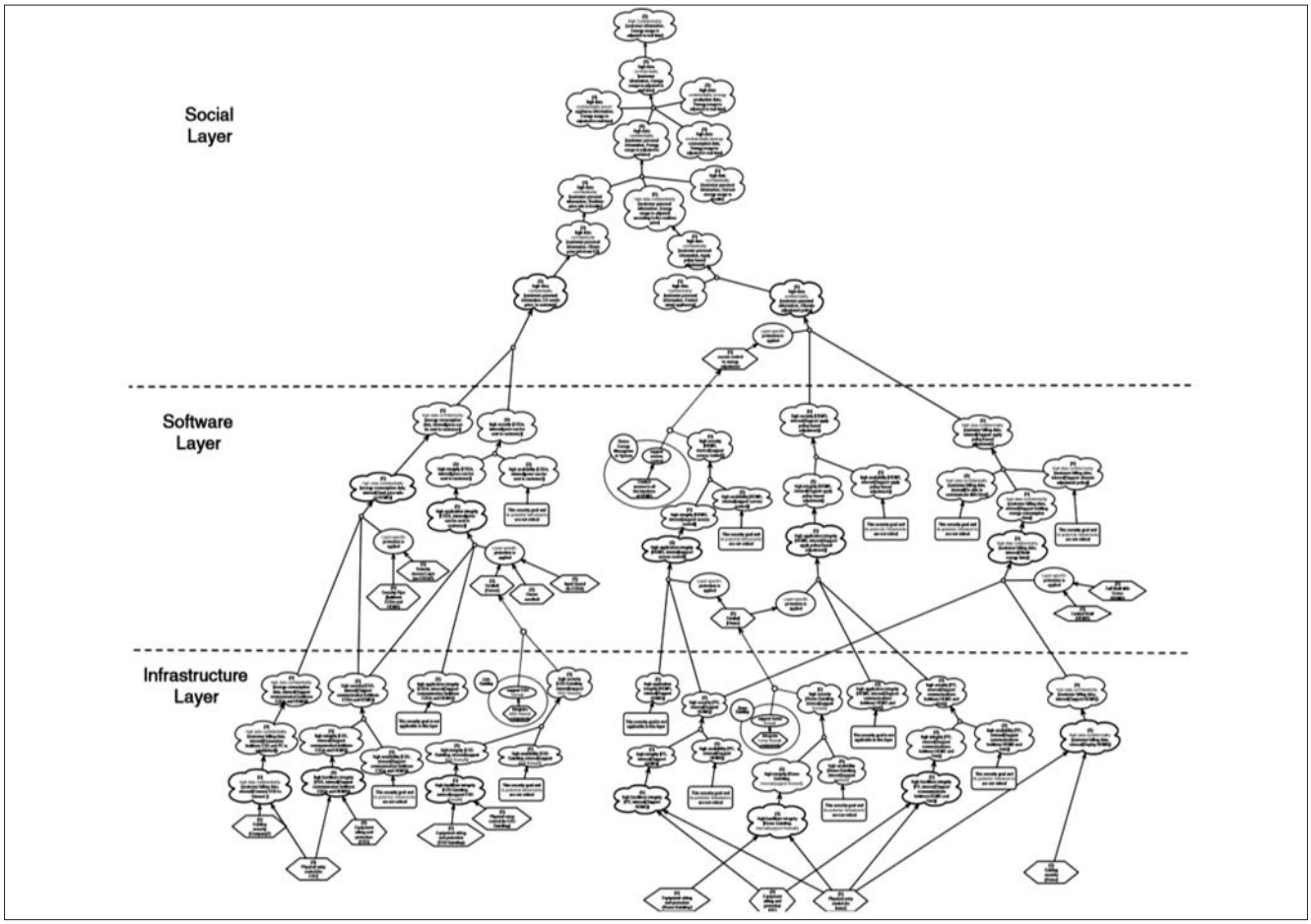
- لایه اجتماعی: دیواره آتش، Security Pipe (میان ESSA و HEMS), Server sandbox, Limited View (HEMS)
- لایه زیرساخت: امنیت کابل کشی، Equipment sitting and protection (PC), Equipment sitting and protection (Home Gateway), Equipment sitting and protection (ESS), Cabling security (Company2)

۴-۲-۱- ارزیابی

• درطول این تحلیل در چندین جا به تخصص امنیت نیاز است (پاسخ به RQ1.2.1) (در حین تحلیل ساده‌سازی، تحلیل الگوی امنیت).

• پالایش هدف امنیتی در لایه اجتماعی پیچیده تر و سخت تر از تحلیل در سایر لایه‌هاست زیرا تحلیل‌های دستی بیشتری دارد (پاسخ به RQ1.2.2) در این لایه تحلیل از یک هدف امنیتی سطح بالا شروع می‌شود که ذاتا گسترده بوده و منعکس کننده نیازهای واقعی سودبران نیست. در لایه‌های بعدی اهداف امنیتی ریشه از ملاحظات امنیتی لایه‌های بالاتر نشئت می‌گیرند که قبلا مشخص شده شامل نیازهای دقیق سودبران می‌باشند.

• انجام تحلیل روی فرانامه شش ساعت به طول انجامیده (پاسخ به RQ1.2.3)، نتیجه گرفته می‌شود که این روش می‌تواند به‌صورت اثربخش و در ارتباط با تحلیل جامع نیازمندی‌های امنیتی سیستم‌های



شکل ۱۸: مدل جامع هدف امنیتی

مقیاس وسیع به‌کار گرفته شود (پاسخ به RQ1.2).

• در تحلیل فرانامه ۲۱ راه‌حل امنیتی جامع تولید شد (پاسخ به RQ2.2) که هریک شامل راه‌حل‌های خاصی بوده و محافظت امنیتی در هر سه لایه را فراهم می‌آورد (پاسخ به RQ2.1)

• دو عامل وجود دارند که کیفیت نتایج تحلیل را تحت تاثیر قرار می‌دهند و باید در کارهای آینده بهبود داده شوند(RQ2.3):

-۱ فهرست الگوهای امنیتی مستقیما روی راه‌حل‌های امنیتی که در انتهای تحلیل امنیتی تولید می‌شوند تاثیر دارد. -۲ وجود مجموعه جامعی از تهدیدات برای تضمین کامل بودن تحلیل مهم است.

بنابر پاسخ داده شده به پرسش‌های پژوهش ادعا می‌شود که تحلیل امنیتی ارائه شده پوشش خوبی روی ملاحظات امنیتی داشته و می‌تواند به‌صورت موثر در محافظت امنیتی جامع از سیستم‌های مقیاس بزرگ شرکت نماید (RQ2)

۵- مزایای چارچوب پیشنهادی

۱- هدایت سامانمند تحلیل‌گر از طریق یک فرآیند تحلیل جامع امنیت که لایه‌های مختلف یک STS را پوشش می‌دهد. (پیوندهای پشتیبانی برای مرتبط ساختن تحلیل در میان لایه‌ها بسیار مهم است)

۲- قابلیت شناسایی راه‌حل‌های امنیتی جامع، از آن جایی که پیاده‌سازی راه‌حل‌های جامع امنیتی به نظر پرهزینه هستند، شناسایی و ارزیابی تمام جایگزین‌های پیش رو از اهمیت ویژه‌ای برخوردار خواهد بود تا تحلیل‌گران بتوانند مناسب‌ترین راه‌حل را با توجه به بودجه خود انتخاب کنند.

۶- انعطاف‌پذیری‌های چارچوب

۱- تغییر تعداد و محتوای لایه‌ها براساس زمینه کاربرد، مثلا حذف لایه اجتماعی برای سیستم‌های تکنیکی چون سیستم‌های سایبری-فیزیکی یا اضافه کردن لایه سیستم عامل میان لایه زیرساخت و کاربرد

۲- استفاده از روش تحلیل پایین به بالا به جای روش بالا به پایین

۳- گسترش چارچوب با ادغام یکپارچه پیشرفت های اخیر در روش‌های تحلیل تهدید برای پشتیبانی از تحلیل ساده‌سازی اهداف امنیتی

۷-استفاده مجدد از دانش امنیت

با توجه به پیچیدگی و ناهمگونی ذاتی STSها، تحلیل جامع امنیت

دربرگیرندۀ طیف وسیعی از موضوعات امنیتی است که نیازمند دانش زیـادی در حوزۀ امنیت می‌باشـد و این موضـوع تحلیل را پیچیده‌تر نیز می‌سازد. از طرف دیگر کسـب دانش امنیتی کار ساده‌ای نیست. بنابراین برای پاسـخگویی به این چالش، رویکرد به‌کارگرفته شده در توسـعۀ این چارچوب توجه ویژه‌ای به استفاده مجدد از دانش داشته تا این تحلیل دانش فشـرده تسهیل شود. اقدامات زیر در راستای این هدف انجام گرفته‌اند:

۱- کپسـوله کردن بخشـی از دانش امنیتی موردنیاز در قالب قواعد اسـتنتاجی متناظر. این قواعد مستقل از دامنه کاربرد هستند و برای تمام انواع سیسـتم‌ها قابل اسـتفاده می‌باشـند. یکی از کارهایی که می‌توان در آینده انجام داد ایجاد قواعد خاص دامنه است.

۲- اسـتفاده مجـدد از الگوهـای امنیتی در تولید موثـر راه‌حل‌های امنیتی ثابت شده‌ای که اهداف امنیتی را عملیاتی می‌سازند. بنابراین نتایج تحلیل بسـتگی به کاتالوگ الگوهای امنیتی به‌کارگرفته شـده دارد. اگرچه اسـتفاده مجدد از این الگوها تحلیل را ساده می‌سازد اما لازم است تحلیل‌گر قبل از استفاده درک کاملی از آن ها داشته باشد.

نگاشت میان چارچوب سه لایه و چارچوب‌های معماری سازمانی

چارچوب‌های معماری سازمانی اولین بار توسط جان زکمن و با هدف هم راسـتایی موثر نیازمندی‌های کسـب‌وکار با سیستم‌های IT مورد بررسی و پژوهش قرار گرفتند. چارچوب زکمن یک طبقه‌بندی جامع از آرتیفکت‌های یک سازمان ارائه می‌دهد. این آرتیفکت‌ها از دو جنبۀ دیدگاه کاربر (مثلا مالک کسـب‌وکار) و تمرکز توصیف (مثلا کاربرد) تعریف می‌شوند. براسـاس این طبقه‌بندی چارچوب معماری Open Group (توگـف) معماری سـازمانی را به ۴ طبقه تقسـیم می‌کند: معماری کسـب‌وکار، معماری داده، معمـاری کاربرد و معماری فنی. اگرچه این مدل‌های معماری سـازمانی آرتیفکت‌های سـازمان را در لایه‌های مختلف مدل می‌کنند اما برای تحلیل راه‌حل‌های امنیتی در میان لایه‌ها راهکاری ندارند.

چارچـوب پیشـنهادی و چارچوب توگف می‌تواننـد یکدیگر را کامل کنند. از یک سـو طبقه‌بندی‌های تعریف شده در توگف را می‌توان با چارچوب سـه لایه نیازمندی‌ها تطبیق داد و از این طریق ساخت این چارچوب سه لایه را تسهیل کرد. معماری کسب‌وکار به لایه اجتماعی نگاشت می‌شود، هر فعالیت کسب‌وکار در معماری کسب‌وکار به‌عنوان یک وظیفه (task)کسـب‌وکار مدل‌سـازی می‌شـود. معماری کاربرد بـا لایه نرم‌افزار متناظر اسـت، تابع کاربرد به‌عنـوان یک کار(task) کاربردی مدل‌سازی می‌شود. معماری فنی با لایه زیرساخت مطابقت دارد و به تحلیل‌گر کمک می‌کند که کارهای اسـتقرار را در این لایه شناسـایی کند. از سوی دیگر، با دردسـترس بودن معماری توگف و براسـاس نگاشـت فوق تحلیل‌گر قادر خواهد بود مدل‌های سـه لایه نیازمندی‌های عملکردی را به روش پایین به بالا و با پرسیدن سوالات «چرا» ایجاد کند.

منبع

- Li, T., Horkoff, J., Mylopoulos, J.: Holistic security requirements analysis for socio-technical systems (REFSQ 2016). Softw Syst Model

خوانش انتقادی طرح قانونی تشکیل سازمان نظام مهندسی ارتباطات و فناوری اطلاعات (نمافا)

سید ابراهیم ابطحی
استادیار دانشکده مهندسی کامپیوتر- دانشگاه صنعتی شریف
نایب رئیس انجمن انفورماتیک ایران
abtahi@sharif.edu

مقدمه (دلایل توجیهی)

طرح تشکیل سازمان نظام مهندسی ارتباطات و فناوری اطلاعات (نمافا) که به امضای ۳۶ نفر از نمایندگان رسیده است در جلسه علنی مورخ ۹۸/۱۱/۸ مجلس شورای اسلامی به شرح زیر اعلام وصول گردید. در مقدمه این طرح آمده است: از آنجا که حوزه ارتباطات، فناوری اطلاعات و فضای مجازی اعم از نرم‌افزاری، تولید محتوا، سخت‌افزاری، شبکه، اینترنت، مدیریت و مهندسی فناوری اطلاعات و ارتباطات، هوشمندسازی ابنیه، اقتصاد دیجیتال، کسب و کارهای نوین، شرکت‌های نوپای فضای مجازی، مهندسی فضای مجازی و سایر رشته‌های مرتبط که امروزه در تمام بخش‌های اقتصادی- اجتماعی، فرهنگی- سیاسی و امنیتی مؤثر می‌باشد و واحدهای مختلف اعم از اتحادیه‌ها و مؤسسات دولتی و غیردولتی مختلف مسئولیت موارد مذکور را دارند و گاهی هم‌پوشانی و بعضاً خلأ مدیریتی دارد لازم است که تحت یک سازمان واحد ساماندهی و به‌صورت غیردولتی به‌صورت هزینه- درآمد اداره می‌گردد و هیچ‌گونه بار مالی برای دولت نخواهد داشت.

لذا طرح ذیل جهت حل این مشکلات به مجلس شورای اسلامی تقدیم می‌شود: اسامی ۳۶ نماینده پیشنهاد دهنده مجلس

متن و مواد تشکیل دهنده طرح تشکیل سازمان نظام مهندسی ارتباطات و فناوری اطلاعات (نمافا)

ماده ۱- «نظام صنفی رایانه‌ای» موضوع ماده(۱۲) قانون حمایت از حقوق پدیدآورندگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۷۹/۱۰/۴ به «سازمان نظام مهندسی ارتباطات و فناوری اطلاعات(نمافا) » ارتقاء می‌یابد که در این قانون از آن به «سازمان» یاد می‌شود.

ماده ۲- «سازمان»، نهادی مستقل، غیرانتفاعی و غیردولتی و متشکل از ارکان ذیل است:

سازمان‌های نمافای هر استان، شورای انتظامی هر استان، هیئت عمومی سازمان، شورای مرکزی سازمان، شورای انتظامی کل، بازرس و رئیس سازمان با مشارکت اعضای:

الف- حقوقی شامل شرکت‌ها، تعاونی‌ها و مؤسسات دارای موضوع فعالیت در رشته‌های مرتبط یا زمینه ارتباطات و فناوری اطلاعات

ب- حقیقی شامل صاحبان فروشگاه‌های دارای پروانه کسب، فارغ‌التحصیلان دانشگاهی و دارندگان مهارت تخصصی مرتبط

ماده ۳- هیئت مدیره نمافای سازمان استان‌ها با رأی اعضای دارای مجوز فعالیت معتبر نمافای استان، و اعضای شورای مرکزی با رأی هیئت عمومی نمافای هیئت مدیره‌های استان‌ها، وفق مفاد آیین‌نامه اجرائی این قانون انتخاب می‌شوند.

ماده ۴- انتخابات مجمع عمومی سازمان نظام‌های استانی با رأی‌گیری از کلیه اعضای حقیقی متناسب با رتبه عضویت و اعضای حقوقی با حق رأی معادل حق رأی تمامی کارکنان عضو حقوقی با عضویت در سازمان هر سه‌سال یک مرتبه انجام می‌گیرد.

ماده ۵- وظایف و اختیارات سازمان به‌شرح ذیل است:

۱- صدور مجوز فعالیت تأسیس، رده‌بندی تنظیم و تنسیق امور،

نظارت، بازرسی و رسیدگی به تخلفات افراد و واحدهای صنفی که در کلیه زمینه‌های تجاری رایانه‌ای مجاز، فاوا و کسب و کار مبتنی بر فضای مجازی فعالیت می‌کنند.
۲- صدور مجوز تأسیس و نظارت بر فعالیت تشکل‌ها و اتحادیه‌های منطقه‌ای و بین‌المللی در زمینه فعالیت‌های موضوع این قانون
۳- دریافت تقاضای ثبت، رده‌بندی و ثبت حقوق مادی و معنوی نرم‌افزارها و برنامه‌های رایانه‌ای و محتوای دیداری، شنیداری و نوشتاری
۴- ارائه نظرات مشورتی، مشارکت و همکاری با قوای سه‌گانه، دستگاه‌های اجرائی وابسته و سایر مراجع ذی‌ربط در زمینه وظایف قانونی دستگاه‌ها و مراجع مزبور و اجرائی قوانین و مقررات موضوعه در حدود فعالیت‌های موضوع ایجاد سازمان
۵- سایر اقدامات در زمینه توسعه و رفع موانع فعالیت‌های موضوع بند(۱) و صیانت از حقوق اعضاء، تأمین منافع و رفاه اعضاء
۶- برگزاری دوره‌های آموزشی و بازآموزی اعضاء ونظام رتبه‌بندی مهارت‌های موضوع فعالیت‌های سازمان

ماده ۶- هزینه‌های سازمان از محل ورودیه‌ها و حق عضویت پرداختی اعضاء، معادل دو در ده هزار از درآمد اعضاء، کمک‌های اعطائی، فعالیت‌های پژوهشی و مشاوره‌ای و برگزاری همایش‌ها و نمایشگاه‌ها تأمین می‌شود.

ماده ۷- نحوه صدور مجوز فعالیت و تنظیم و تنسیق امور واحدهای زیرنظر سازمان به‌شرح ذیل است:
۱- سازماندهی و نظم بخشی فعالیت‌های تجاری مجاز رایانه‌ای، فناوری اطلاعات و ارتباطات و فضای مجازی توسط سازمان نمافای استان‌ها با بررسی تقاضای واجدین شرایط عضویت با صدور و تحویل مجوز فعالیت به انجام می‌رسد.
تبصره- در این قانون مجوز فعالیت به مجوزی گفته می‌شود که طبق مقررات این قانون به‌منظور شروع و ادامه کسب‌وکار یا حرفه به‌صورت موقت یک‌ساله یا دائم پنج‌ساله با ذکر مشخصات اصلی شخص حقیقی یا حقوقی، رشته تخصصی و رتبه یا میزان تجربه یا تخصص به فرد صنفی حقیقی یا حقوقی برای محل با نشانی فیزیکی و یا آدرس اینترنتی با دامنه ir (دامنه معتبر کشوری نظیر IR و ایران) مشخص و معیّن توسط سازمان نمافای استان صادر و تحویل می‌شود.
۲- افراد حقیقی و حقوقی صنفی حوزه فناوری اطلاعات و ارتباطات موظفند قبل از شروع به فعالیت صنفی یا اشتغال به کسب و حرفه در این زمینه، نسبت به أخذ مجوز فعالیت از سازمان نمافای استان اقدام نمایند.
۳- هرگونه اشتغال و فعالیت تخصصی، تجاری و اقتصادی در زمینه‌های تعیین‌شده در این قانون منوط به عضویت و اخذ مجوز شروع فعالیت از سازمان نمافای استان است.
۴- اشخاص حقوقی برای عضویت در سازمان باید در موضوع فعالیت مندرج در اساسنامه معتبر خود عناوین و موضوعات مطابق با چهارچوب و اهداف این قانون را دارا باشند.
۵- اشخاص حقیقی برای عضویت در سازمان باید مدارک تحصیلی مرتبط دانشگاهی (حداقل کارشناسی تخصصی) در رشته‌های اصلی یا زمینه مهندسی کامپیوتر، فناوری اطلاعات و ارتباطات و یا مدارک مرتبط با مهارت‌های حرفه‌ای مورد پذیرش این سازمان برای عضویت و دریافت مجوز فعالیت ارائه نمایند. معرفی و به‌روزرسانی رشته‌های دانشگاهی ومهارت‌های مورد تأیید توسط شورای اجرائی فناوری اطلاعات (با وزارت ارتباطات و فناوری اطلاعات) انجام می‌شود.

ماده ۸- نظارت و بازرسی فعالیت‌های مجاز رایانه‌ای، فناوری اطلاعات و ارتباطات و فضای مجازی اعم از اعضای تحت پوشش یا فعال غیرمجاز فاقد پروانه یا مجوز اشتغال توسط واحد بررسی و نظارت سازمان نمافای استان‌ها انجام می‌شود.

ماده ۹- افراد صنفی مکلفند قوانین ومقررات صنفی، انتظامی و دستورالعمل‌های مربوط به نرخ‌گذاری کالاها و خدمات و همچنین مقررات و ضوابط رعایت حقوق مصرف‌کنندگان را که از سوی مراجع قانونی‌ذی‌ربط ابلاغ می‌گردد، رعایت و اجرا کنند. در صورتی که در نتیجه بازرسی و نظارت مستمر و یا وصول شکایات افراد صنفی تحت پوشش این قانون، مرتکب تخلفات صنفی شوند شورای انتظامی (بدوی) استان، حسب گزارش واحد بازرسی و نظارت سازمان یا شکایات واصله به تخلفات صنفی آن‌ها رسیدگی و در صورت اثبات تخلف، متناسب با میزان تخلف صورت‌گرفته به مجازات یا محرومیت‌های صنفی درجه ۱ تا ۵ محکوم خواهند شد که محرومیت‌های درجه ۱ تا ۳ حداکثر تا پانزده روز پس از صدور رأی، در شورای انتظامی تجدیدنظر استان قابل تجدیدنظرخواهی خواهد بود و محرومیت‌های درجه ۴ و ۵ تا یک‌ماه پس از صدور در شورای انتظامی کل قابل تجدیدنظرخواهی‌خواهد بود.
تبصره- نیروی انتظامی جمهوری اسلامی ایران و سایر ضابطین مشخص‌شده در قوانین مجری اجرای احکام صادر شوراهای انتظامی سازمان می‌باشند.

ماده ۱۰- شورای انتظامی استان به‌منظور رسیدگی به شکایات اشخاص حقیقی و حقوقی در خصوص تخلفات حرفه‌ای، انضباطی و انتظامی اعضاء متشکل از دو یا چهار نفراز اعضای حقیقی به معرفی هیئت مدیره نظام استانی و یک نفر حقوقدان می‌باشد و همگی با حکم رئیس شورای مرکزی نظام برای مدت سه‌سال منصوب می‌شوند.

ماده ۱۱- چگونگی رسیدگی به تخلفات و تعیین مجازات‌های انضباطی و موارد قابل‌تجدیدنظر در شورای انتظامی نظام طبق مواد آتی و یا مفاد آیین‌نامه اجرائی مرتبط خواهد بود. شورای انتظامی استان اگر شکایتی را وارد نداند و یا رسیدگی به شکایتی را در صلاحیت خود تشخیص ندهد نظر به رد شکایت یا عدم‌صلاحیت داده و در غیر این‌صورت پس از اخذ دفاعیات اتخاذ تصمیم می‌کند. شورا در صورت نیاز از طرفین برای استماع اظهارات‌آنان دعوت نماید. عدم حضور شاکی یا وکیل یا نماینده او در اولین جلسه رسیدگی بدون اعلام قبلی در حکم انصراف از شکایت است، لیکن عدم حضور مشتکی‌عنه

مانـع رسـیدگی و أخذ تصمیم نخواهـد بود. در صورت درخواسـت مشتکی‌عنه جهت حضور، شورا موظف به دعوت از وی می‌باشد.
مشـتکی‌عنه درصورت عدم امکان حضور، لایحه دفاعیه خود را قبل از جلسه رسـیدگی به دبیرخانه شورای انتظامی استان تسلیم یا یک نفر را به‌عنوان وکیل معرفی می‌نماید. آرای شـورای انتظامی باید مستند و مستدل و صریح بوده و در ذیل برگ رأی، نحوه اعتراض و مهلت آن را به‌طور دقیق ذکر شود.
ماده ۱۲- مجازات‌های انتظامی مربوط به تخلفات صنفی به‌شرح ذیل است:
درجه۱- اخطار شـفاهی بدون درج در پرونده عضویت در نظام صنفی رایانه‌ای استان
درجـه۲- توبیـخ کتبی یـا درج در پرونده عضویـت در نظام صنفی رایانه‌ای استان
درجه۳- محرومیت موقت از فعالیت صنفی به مدت یک روز تا سه‌ماه
درجه۴- محرومیت موقت از فعالیت صنفی به مدت سه‌ماه و یک روز تا یک‌سال
درجـه۵- محرومیت موقت از فعالیت صنفی به مدت یک‌سـال و یک روز تا پنج‌سال
تبصره- شـورای انتظامی اسـتان می‌تواند برای محرومـان از فعالیت صنفی، الزام انتشـار رأی محرومیت در وبگاه یا درگاه(پورتال) (محروم) را برای تخلفات با درجه محرومیت ۲ تا ۵ ایجاد نماید. در صورت امتناع محروم از انتشار رأی محرومیت در محل تعیین‌شده از وبگاه، محرومیت شـدیدتر با تأکید بر انتشار و آگهی رأی صادره و همچنین الزام انتشار آگهی در درگاه(پورتال)های ساماندهی دولتی به آنجا خواهد رسید.
ماده۱۳- تخلفـات انتظامـی و انضباطی افراد صنفـی و مجازات‌های مربوط حسب مورد با توجه به شرایط، دفعات و مراتب تخلفات به‌شرح جدول زیر می‌باشد.

شماره	عنوان تخلف انتظامی و انضباطی	مجازات
۱	عدم رعایت شئونات شغلی و حرفه‌ای مربوط	درجه ۱ تا ۲
۲	سهل‌انگاری و یا عدم رعایت اصل فنی به نحوی که موجب تضییع حقوق غیر گردد به تناسب میزان خسارات وارده	درجه ۱ تا ۳
۳	صدور تأییدیه‌های خلاف واقع	درجه ۱ تا ۵
۴	ارائه صورت وضعیت یا سایر اوراق و مدارک که موجب تضییع حقوق دیگران شود	درجه ۲ تا ۴
۵	امتناع از انجام تمام یا بخشی از تکالیف ناشی از قرارداد	درجه ۱ تا ۳
۶	جعل و تزویر در اوراق و اسناد و مدارک حرفه‌ای	درجه ۳ تا ۵
۷	اشتغال درکارهایی خارج از صلاحیت حرفه‌ای و یا ظرفیت اشتغال تعیین‌شده توسط مراجع ذی‌ربط	درجه ۳ تا ۵
۸	سوءاستفاده از عضویت و یا موقعیت‌های شغلی و اداری نظام به نفع خود و یا غیر	درجه ۳ تا ۵
۹	دریافت و پرداخت هرگونه مال یا وجه یا قبول خدمت خارج از ضوابط	درجه ۳ تا ۵
۱۰	عدم رعایت مقررات و ضوابط مصوب نظام	درجه ۱ تا ۳
۱۱	تأسیس هرگونه مؤسسه، دفتر یا محل کسب و پیشه برای انجام خدمات فنی بدون داشتن مجوز قانونی لازم	درجه ۲ تا ۵
۱۲	انجام فعالیت در دوره محرومیت موقت، علاوه بر محدودیت سابق	درجه ۴ تا ۵

ماده۱۴- فرد حقیقی یا حقوقی در دوره محرومیت موقت صنفی مجاز به شـرکت در معاملات دولتی و خصوصی اعم از طریق فراخوان‌های عمومی و خصوصی مناقصه برخط یا غیر برخط، مزایده‌ها، مشـارکت عمومی- خصوصی و مسابقه‌ها نخواهد بود.
ماده۱۵- تشخیص تخلف و انطباق آن با هر یک از مجازات‌های مقرر به‌عهده شـورای انتظامی استان است وتکرار تخلف از هر نوع که باشد موجب مجازات شـدیدتر خواهد بود. ارتکاب جرائم متعدد مشـمول جمع مجازات‌ها است که درهر حال مجموع محرومیت بیش از ده‌سال نخواهد بود.
ماده۱۶- آیین‌نامه اجرائی این قانون، اساسـنامه سازمان و اساسنامه الگوی نمافاهای اسـتانی توسـط وزارت ارتباطات و فناوری اطلاعات با همکاری وزارت فرهنگ و ارشـاد اسلامی و سازمان برنامه و بودجه ظرف مدت دو سـال تهیه شـده و به‌تصویب هیئت وزیران می‌رسـد. تا زمـان تصویب و ابلاغ آن‌هـا «آیین‌نامه اجرائی مـواد (۲) و (۱۷) قانـون حمایت از حقوق پدیدآورنـدگان نرم‌افزارهای رایانه‌ای مصوب ۱۳۸۳/۴/۲۱ هیئت وزیران»، معتبر و لازم‌الاجرا است.

خوانش انتقادی طرح

در این نوشـته با اشـاره به پیشینه و مدل رایجی برای این نظامات، بـه ایرادی بنیادی در خلط جایـگاه منفک نظامات اجرائی که به نظر می‌رسـد پیشـنهاد دهندگان طرح به آن کم توجهی نشـان داده‌اند، اشاره می‌کنیم که امیدواریم در مرحله رایج اصلاحات ماقبل تصویب، مورد توجه قرار گیرد.
پیشـینه این طرح به بیست سـال پیش بر می‌گردد که شورای عالی انفورماتیک کشـور در سال ۱۳۷۹ به شرکت راهگشای سامانه تهران، پیشـنهاد تهیـه طرح نظارت بـر پروژه‌های انفورماتیکـی را داد. این طرح به شـکل جامعی تهیه شـد و شامل پیشـنهادی برای تشکیل نظام مهندسـی انفورماتیک در فصل ششـم بود. نگارنده که در تهیه این طرح نقش فنی مسـتقیم داشته اسـت به یاد دارد که در جلسه ارائـه نتایج این طـرح با حضور نمایندگان شـرکت‌های نرم‌افزاری به دعوت شـورای عالی انفورماتیک در همان سـال، مواجهه نامنتظری با آن صـورت گرفت. یعنی اکثریتی به تهیـه کنندگان طرح تاختند و ایـن امر را کاری غیرضروری و مداخلـه جویانه در امر خلاقهٔ تولید نرم‌افزار و دشواری‌ساز برای آن تلقی کردند. البته همان زمان نگارنده که به دوسـتان توضیح داد، تصور کار هنری از تولید نرم‌افزار مربوط به گذشـته است و امروز(آنروز) کاری مهندسـی تلقی شده و نیاز به نظارت در تولید و تحویل دارد. متاسـفانه عدم پذیرش این اسـتدلال منطقی این طرح را به محاق فراموشی سبرد. تا شش سال بعد که در سـال ۱۳۸۵ مجددا با عطف به سوابق و برحسب نیاز، مرکز تحقیقات مخابرات ایران به‌عنوان بازوی پژوهشـی انفورماتیک کشـور از همان شـرکت خواست طرح نظام مهندسـی فناوری اطلاعات را پژوهش و

تهیــه کند . در میانه نزدیک به پایان کار، مرکز از پیمانکار خواســت نظام را به ارتباطات هم تسری دهد که موجب بازبینی گسترده‌ای در طرح، در پایان مراحل تدوین شــد. این طرح بــا عنوان نظام فناوری اطلاعات و ارتباطات در کشور هم، در مرکز، نوشته باقی ماند و تحقق نیافت. در ســایه اقدامات عجیب و نســنجیده مجریان دولتی، به‌ویژه در نیمــه دوم دهه هشــتاد و نیمه اول دهه نود، بر مشــکلات بخش انفورماتیک کشــور به تبع حضور گروهی، کمتر کاردان در بســیاری عرصه‌ها به‌ویژه از بعد دیوان سالاری، افزوده شد. به یکباره با شوراهای اداری متعــددی در این بخش، بدون تفکیک وظایف و علت وجودی، مواجه شــدیم که مسئولان به ناچار در اقدامی کمتر سنجیده، دستور ادغام آن‌ها را دادند. بر این دشواری باید بی‌تدبیری دیگری را هم برای ثبت در پیشــینه، اشــاره کرد و آن حذف ناگفته ولی ضمنی مراحل نسبتا شفاف برگزاری مناقصه‌های دولتی پروژه‌های رایانه‌ای بود که به قولی منجر به تعطیلی حدود چهل درصد شــرکت‌های فعال رایانه‌ای در آن دوران و بیــکاری و مهاجرت ناگزیرگروهی از کارشناســان این رشته گردید.

در این میان با معلق شدن فعالیت‌های شورای عالی انفورماتیک کشور که قدیمی ترین شــورای دولتی در حــوزه انفورماتیک پس از انقلاب بــود، وظیفه ثبت نرم‌افزار در حمایــت از قانون حق تکثیر محصولات نرم‌افزاری به نظام نوپای صنف رایانه کشــور که نظامی صنفی مصرح در نام خود بود، ســپرده شــد .ســپردن یــک وظیفه فنــی، علمی و مهندســی به نظامی که خود ســودبر اصلی در این زمینه است، کاری غیر اصول و غیر علمی بود. همزمان، هر چند با تاخیر بســیار، مفهوم حرفه‌ای‌گری و نظام حرفه‌ای در حوزه کامپیوتر در کشــور مطرح و با اقدامی عجولانه و بدون پیش بینی مقدمات لازم، آزمون حرفه‌ای‌گری در این رشــته، در ردیف فعالیت‌های دیگر به مرکز ســنجش آموزش کشور و طراحی ســوالات آن به استادان دانشگاهی این رشته سپرده شــد. این دو اقدام با توجه به مفهوم حرفه‌ای‌گری مهندسی و راه‌های اقدام آن، هر دو ناصواب به‌نظر می‌رسید. به همین دلیل در دوره اول آن تنها تعداد معدودی به اندازه‌ای کمتر از تعداد انگشــتان دو دست، داوطلب آزمون و همگی مردود شدند. در دوره‌های بعد هم داوطلبان زیادی از این آزمون اســتقبال ننمودند. زیرا اولا فرهنگ‌ســازی لازم در معرفی مفاهیــم و منطق حرفه‌ای‌گــری در حوزه‌های گوناگون از جمله مهندســی رایانه بین عموم به‌ویژه دانشگاهیان شامل استادان و دانشــجویان صورت نگرفته بود. ثانیا این امر به وزارت علوم، تحقیقات و فناوری که نماد نظام علمی اســت، سپرده شد، نه به نظام حرفه‌ای ناموجود، که به آن ربطی نداشــت. استادان رشته رایانه هم در بیشتر موارد ســوالات این آزمون را چون ســوالات آزمون ورودی دوره‌های کارشناسی ارشد رایانه، طراحی می‌کردند که خطای مضاعفی بود.

در اینجا برای روشن کردن موضوع اجازه دهید به بحث مختصری در مورد حرفه، حرفه‌ای گری و نظامات حرفه‌ای وظایف و کارکردهایشان به‌ویژه در حوزه رایانه بپردازیم. حرفه انجام کار شاغل با کمینه کیفیت لازم اســت که به آن استاندارد حرفه می‌گویند. این استانداردها حرفه را یــا عرف جامعه یا نظام حرفه‌ای آن رشــته، تعییــن می‌کند. برای رشــته مهندســی، حرفه‌ای دانش‌آموخته دانشــگاهی رشته ای است کــه با آزمونی،کمینه ســواد و دانش لازم او ســنجیده می‌شــود و در صورت پذیرش، در دوره‌های آموزشــی با اخــلاق رایج، آداب، حقوق، قوانین، آئین نامه‌ها و اســتانداردهای انجام کار ملی و جهانی توســط مهندســان پیشکسوت حرفه‌ای آشنا شده و با گرفتن مجوز انجام کار در سطح اولیه خبرگی و تجربی آماده حضور در بازار کار می‌شود. بعد از آن، سالیانه توسط نظام حرفه‌ای در رشته خود نوآموزی و بازآموزی می‌شــود و با امتحانات ادواری با تمدید یا ارتقای مجوز، مراحل بلوغ حرفــه‌ای را طی می‌کند. حمایت مهم نظــام حرفه‌ای، از فرد یا بنگاه حرفــه‌ای، حمایت قضائی در موارد اقدامات ســهوی یا در حد وســع، اما متاســفانه آسیب‌رسانده به سودبرانی (ذینفعانی) است که شاکیان احتمالــی فرد حرفه‌ای پس از بروز نتایج اقدامــات او بوده‌اند. در این موقعیت‌ها، کمیته‌های انتظامــی نظامات حرفه‌ای، ماقبل قوه قضائیه قرار می‌گیرند و تشــخیص فنی قصور عمدی احتمالی به آنان سپرده می‌شــود و در صــورت عدم احراز آن، حکم برائــت از خطا، همین جا صادر شده و شکایت بدون ارجاع به قوه قضائیه مختومه می‌شود. این حمایت، انجام کار حرفه‌ای را تســهیل و تسریع می‌کند. در عین حال از بار کاری قوه قضائیه می‌کاهد و برای انبوه حرفه‌ای‌های درســتکار، آرامــش در انجــام کار را فراهــم می‌کند. امروزه کــه رایانه و فناوری اطلاعات با زندگی عجین شــده و به قولی، ســبک زندگی انسان‌ها را می‌سازد، وجود نظام حرفه‌ای برای آن لازم و ضروری به‌نظر می‌رسد. قبــل از اشــاره به ایرادی اساســی که به این طــرح وارد می‌دانیم، بد نیســت توضیح مختصری در مورد نظامات انجام کار و پیوندهای آنان بیان کنیم. بیشینه نظامات حرفه‌ای مرتبط با هر شکل خاص از انجام کار مهندسی را در اجرای چهار نظام علمی، اجرائی، صنفی و حرفه‌ای با تعاملاتشــان دانســته‌اند. تفکیک وظایفی بیــن این نظامات صورت گرفتــه کــه در صورت ادغام، به تناســبات آن‌ها در اجــرا، باید توجه شــود. نکته‌ای که جای آن در طرح مورد بحث ما خالی اســت. نظام علمی معمولا وظیفه آموزش ســرمایه‌های انسانی برای حضور در بازار کار را بــه عهده دارد. نظام حرفه‌ای، دانش آموخته‌های نظام علمی را برای حضور در بازار کار آماده می‌کند. نظام صنفی مســئولیت ثبت و حمایت از حقوق اصناف ثبت شده خود متشکل از حرفه‌ای های نظام حرفــه‌ای را دارد.نظام اجرائی در گونه‌های دولتی و خصوصی به‌عنوان کارفرما، از فعالیت حرفه‌ای های صنوف بهره می‌گیرد.

با این مقدمه نســبتا طولانی به یک ایراد کلیدی در طرح پیشنهادی می‌پردازیــم و خواســتار رفع یا اصــلاح این ابهام هســتیم. در طرح پیشــنهادی، نظامی مهندســی با ترکیبی از وظایــف نظام حرفه‌ای و صنفی و علمی تعریف شــده و اجرای آن بــه عهده نظامی صنفی که در اجرای وظایف خود توانا نیســت گذارده شده تا آن را ارتقا دهد که به‌نظر شدنی نمی‌رسد.

به نام خدا

ITRC

مرکز تحقیقات مخابرات ایران (ITRC)

مرکز نخبگان ICT

(CEICT)

تدوین نظام مهندسی
فناوری اطلاعات و ارتباطات
در کشور

مجری: شرکت راهگشای سامانه تهران
ناظرمستقیم: آقای مهندس جلالی
ناظر اصلی: آقای مهندس هاشمی فشارکی

نسخه ۴
۱۳۸۵/۹/۱۱

تهیه کننده: شرکت راهگشای سامانه تهران
تلفن: ۴-۸۸۸۷۸۷۳۶
پست الکترونیک: info@rahgosha.com

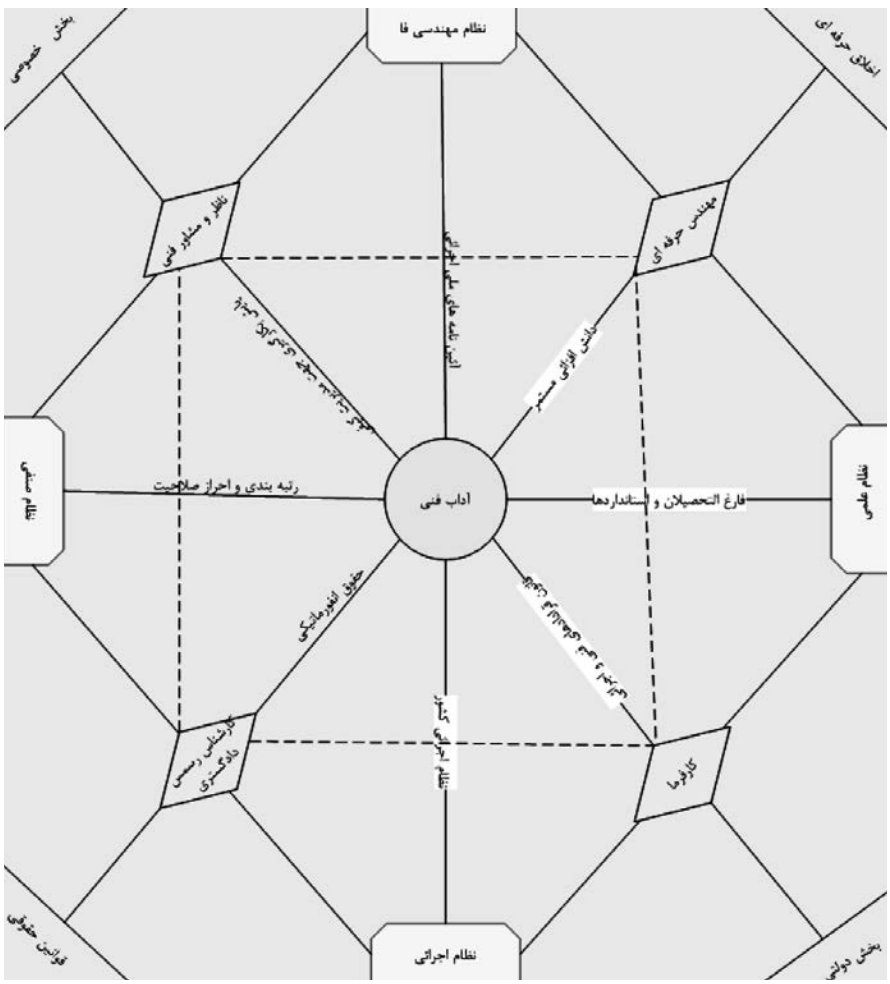
Reference 35

سازمان مدیریت و برنامه‌ریزی
شورای عالی انفورماتیک کشور

نظارت بر
پروژه‌های انفورماتیکی

فصل ششم: نظام مهندسی انفورماتیک ۶۱
۶-۱- اهداف و خط مشی ۷۰
۶-۲- وظایف و مسئولیت ها ۷۲
۶-۳- ساختار و تشکیلات ۷۳
۶-۴- طبقه بندی و احراز صلاحیت ها ۸۳
۶-۵- گردش عملیات و مقررات نظارت ۸۸

مهرماه ۱۳۷۱



مهارت‌های نرم
راهنمای زندگی تولیدکنندگان نرم‌افزار
(قسمت ششم)

ترجمهٔ ابراهیم نقیب‌زادهٔ مشایخ
پست الکترونیکی: mashayekh@isi.org.ir

مقدمهٔ مترجم

سال گذشته، آقای احسان ریحانی‌منش، از اعضای گرامی انجمن انفورماتیک ایران، با ارسال یک نسخه از کتاب «مهارت‌های نرم: راهنمای زندگی تولیدکنندگان نرم‌افزار» نوشتهٔ جان سانمز، ترجمهٔ آن را به من پیشنهاد کرد. در تعطیلات نوروز امسال، فرصتی شد تا به خواندن این کتاب جالب بپردازم. عبارت «مهارت‌های نرم»، عبارتی است که به قابلیت‌های ناملموس و غیرفنّی هر کار اشاره می‌کند. در حوزهٔ تولید نرم‌افزار، برخی از این مهارت‌ها عبارتند از تعامل با مشتریان، همکاران و مدیران، یافتن شغل مناسب، به‌دست آوردن امنیت مالی، حفظ تناسب اندام و یافتن عشق واقعی در زندگی.

جان سانمز، نویسندهٔ کتاب، خود تولیدکنندهٔ نرم‌افزار، مدرّس و فردی است که به برنامه‌نویسان و مهندسان نرم‌افزار در دستیابی به هدف‌هایشان در زندگی کمک می‌کند. وی همچنین بنیان‌گذار بزرگ‌ترین وب‌نوشت برنامه‌نویسان در اینترنت Simple programmar.com است. کتاب مهارت‌های نرم که در سال ۲۰۱۴ انتشار یافته، یکی از پرفروش‌ترین کتاب‌ها در رده‌بندی وبگاه آمازون بوده است.

ترجمهٔ کتاب «مهارت‌های نرم: راهنمای زندگی تولیدکنندگان نرم‌افزار» به‌صورت یک سلسله مقالهٔ دنباله‌دار تقدیم خوانندگان گرامی گزارش کامپیوتر می‌گردد و امیدوارم کلّ کتاب نیز تا پایان سال از طرف انجمن انفورماتیک ایران منتشر گردد.

من از خواندن این کتاب بسیار لذّت بردم و حیفم آمد که آن را با شما به اشتراک نگذارم. امیدوارم برای شما نیز جالب و آگاهی بخش باشد.

از آقای ریحانی‌منش به خاطر معرفی این کتاب، صمیمانه تشکر می‌کنم.

* * *

فصل ۱۷- درست کردن سابقهٔ کاری

آیا تا کنون به تعطیلات رفته‌اید و در سرسرای هتل‌ها یا دفاتر گردشگری، بروشورهای رنگارنگ را دربارهٔ جاذبه‌های گردشگری آن ناحیه دیده‌اید؟ آیا تا کنون یکی از آن‌ها را برداشته‌اید و نگاه کرده‌اید؟ اغلب آن‌ها تمام رنگی، در سه صفحه و با طراحی بسیار زیبا هستند. می‌توان گفت که کار زیادی برای طراحی هنری آن‌ها شده تا شما را متقاعد سازند که برای دیدن آن جاذبه‌ها پول خرج کنید.

اکنون آن را با سابقهٔ کاری[1] تولیدکنندگان نرم‌افزار مقایسه کنید: با حروف[2] یکنواخت، یک خط در میان، طولانی، معمولاً دارای غلط‌های املائی و دستوری، با جمله‌بندی و ساختار ضعیف و پر از ادّعاهای غیرقابل اثبات. اشتباه نکنید، هر دو این‌ها جنبهٔ تبلیغاتی دارند و تلاش می‌کنند تا نهایتاً یک نفر برای یک چیز پول خرج کند. در یکی، تبلیغات تلاش می‌کند که شما را به مثلاً ۱۰۰ دلار خرج کردن برای یک تور گردشگری ترغیب کند. در آن یکی، تبلیغات تلاش می‌کند که نظر یک مدیر منابع انسانی را برای خرج کردن ۶۰/۰۰۰ دلار، ۸۰/۰۰۰ دلار یا بیشتر برای استخدام یک تولیدکنندهٔ نرم‌افزار برای یک سال جلب کند.

به نظر من، عاقلانه نیست که یک نفر برای فروش یک چیز ۱۰۰ دلاری این همه کار و تلاش را صرف یک ابزار تبلیغاتی کند، امّا یک نفر دیگر برای فروش یک چیز ۶۰/۰۰۰ دلاری یا بیشتر، چنین نسخهٔ بدساخت و پایین‌تر از استانداردی را ارائه کند. برداشت غلط نکنید. من نمی‌گویم که سابقهٔ کاری شما کم‌ارزش است، امّا اگر شما نیز مانند اغلب تولیدکنندگان نرم‌افزار باشید، احتمالاً کار چندانی برای تهیهٔ سابقهٔ کاری خود نکرده‌اید.

شما نویسندهٔ حرفه‌ای سابقهٔ کاری نیستید

1- resume
2- font

به نظر من سابقهٔ کاری شما زیاد به درد بخور نیست و برای این حرفم هم دلیل دارم. دلیلم هم خیلی ساده است: شما نویسندهٔ حرفه‌ای سابقهٔ کاری نیستید. نوشتن سابقهٔ کاری برای شما جنبهٔ حیاتی ندارد. ولی من به شما تضمین می‌دهم که آن کسی که آن بروشور زیبا را درست کرده تا شما را متقاعد سازد که برای یک تور گردشگری ثبت نام کنید، بروشورها یا سایر مواد تبلیغاتی را برای گذران زندگیش درست کرده است.

و با وجودی که بسیاری از کتاب‌ها و برنامه‌های راهنمای شغلی به شما می‌گویند که چگونه یک سابقهٔ کاری بهتر برای خود درست کنید، امّا از نظر من اهمیتی ندارد. چرا؟ زیرا شما نباید نویسندهٔ حرفه‌ای سابقهٔ کاری بشوید. وقت و استعداد شما تلف می‌شود. نوشتن سابقهٔ کاری، مهارتی است که فقط چند بار در دوران کاری خود از آن استفاده می‌کنید. بنابراین، اصلاً عاقلانه نیست که وقتی هزاران نویسندهٔ حرفه‌ای برای این کار وجود دارند که بهتر از شما این کار را انجام می‌دهند، شما سرمایه‌گذاری سنگینی در این زمینه بکنید.

به این مسئله، این‌گونه فکر کنید: مدیرعامل شرکتی که برایش کار می‌کنید، معمولاً نرم‌افزار نمی‌نویسد، مطمئناً او می‌تواند پشت رایانه بنشیند و یاد بگیرد که چگونه نرم‌افزارهای مورد نیاز برای ادارهٔ شرکت را بنویسد. امّا عاقلانه‌تر این است که شما را استخدام کند تا این کار را برایش انجام دهید. بنابراین، شما چرا باید به جای به خدمت گرفتن یک نفر دیگر، وقتتان را برای یادگیری مهارت‌های نوشتن یک سابقهٔ کاری حرفه‌ای تلف کنید.

یک سابقهٔ کارنویس استخدام کنید

امیدوارم تا به حال توانسته باشم شما را متقاعد کنم که باید یک فرد حرفه‌ای را برای نوشتن سابقهٔ کارتان به خدمت بگیرید. امّا چگونه این کار را انجام دهید؟

تعداد زیادی سابقهٔ کارنویس حرفه‌ای در بازار وجود دارد. با یک جستجوی سریع در اینترنت می‌توانید عدّهٔ زیادی از آن‌ها را بیابید، امّا باید در انتخاب آن‌ها دقّت کنید. نوشتن سابقهٔ کاری برای تولیدکنندهٔ نرم‌افزار، کمی چالش برانگیزتر از نوشتن سابقهٔ کاری برای بسیاری از حرفه‌های دیگر است، زیرا تعداد زیادی اصطلاحات قراردادی[3] و فناوری‌های مرتبط با کار ما وجود دارد.

باید به آگاهی شما برسانم که خدمات سابقهٔ کاری‌نویسی، حداقل بهترین‌هایشان، ارزان نیستند امّا ارزشش را دارند زیرا یک سابقهٔ کاری خوب با کمکی که به شما در سریع‌تر پیداکردن کاری با درآمد بالا می‌کند، هزینه‌اش را جبران خواهد کرد. انتظار هزینه‌ای حدود ۳۰۰ تا ۵۰۰ دلار را برای یک سابقهٔ کاری با کیفیت و حرفه‌ای داشته باشید. باز هم تکرار می‌کنم که هزینهٔ بالایی است، امّا اگر بتوانید با آن، کاری را که فقط ۲ تا ۳ درصد بیشتر درآمد داشته باشید پیدا کنید، به راحتی ظرف یک سال بیشتر از آن به‌دست خواهید آورد.

همچنین، پیش از به خدمت گرفتن یک سابقهٔ کارنویس حرفه‌ای، مطمئن شوید که تمام اطلاعاتی را که آن فرد برای انجام کارش نیاز دارد، در اختیار دارید. شما اگر یک سابقهٔ کارنویس حرفه‌ای را به خدمت بگیرید امّا اطلاعات نادقیق به او بدهید، مثلاً تاریخ‌های دقیق کارهای قبلی‌تان یا شرح دقیق مهارت‌ها و مسئولیت‌هایتان را در اختیارش قرار ندهید، هرگونه پولی که به او بپردازید بی‌فایده خواهد بود. وقتی شما یک سابقهٔ کارنویس حرفه‌ای را به خدمت می‌گیرید، اساساً دو چیز را از او می‌خواهید:

- نوشتن یک سابقهٔ کاری خوب و تأثیرگذار برای تبلیغ خدمات شما و معرفی شما به بهترین شکل.
- آماده‌کردن آن در قالبی زیبا و جذّاب

وظیفهٔ آن‌ها نیست که به دنبال اطلاعات شما بگردند یا آن‌ها را راستی‌آزمایی کنند. شما باید هر چه بیشتر اطلاعات در اختیار آن‌ها بگذارید تا آن‌ها بتوانند آن اطلاعات را گرفته و در قالبی پالایش شده جای دهند تا بازاریابی خدمات شما را به نحو مؤثری انجام دهد.

من حس خوبی از به‌خدمت گرفتن یک نفر برای نوشتن سابقهٔ کارم ندارم

این متداول‌ترین مخالفتی است که وقتی به دیگران توصیه می‌کنم تا فردی را برای نوشتن سابقهٔ کار خود به‌خدمت بگیرند، ابراز می‌کنند. خیلی‌ها فکر می‌کنند به خدمت گرفتن یک نفر برای نوشتن خلاصهٔ سوابق آن‌ها «نادرست» و فریبکارانه است. حس می‌کنند که باید خودشان، سابقهٔ کارشان را بنویسند. من این دیدگاه رادرک می‌کنم- و شما می‌توانید این کار را خودتان انجام دهید- امّا چرا فکر می‌کنید که به‌خدمت گرفتن یک نفر برای نوشتن سابقهٔ کار برای شما با به‌خدمت گرفتن فردی برای طراحی وبگاهتان یا رنگ کردن خانه‌تان فرق می‌کند؟ در واقع، بسیاری از آدم‌های مشهور، نویسندگان ناشناسی را به خدمت می‌گیرند تا برایشان کتاب بنویسند و سپس نام خودشان را به‌عنوان نویسنده روی جلد کتاب درج می‌کنند. نکتهٔ من این است که آنقدرها هم که فکر می‌کنید کار عجیبی نیست. این که همیشه فکر کرده‌اید که تولیدکنندگان نرم‌افزار باید خودشان سابقهٔ کار برای خودشان بنویسند، دلیل درستی آن نمی‌شود. لزومی ندارد که به دیگران بگوئید سابقهٔ کارتان را یک آدم حرفه‌ای نوشته است و سرانجام این که اگر واقعاً با این کار احساس راحتی نمی‌کنید،خودتان سابقهٔ کارتان را بنویسید و کسی را برای «اصلاح و بهبود» آن به خدمت بگیرید.

انجام تلاش بیشتر

عنوان این فصل بیانگر این است که سابقهٔ کارهای سنّتی، یکنواخت و خسته‌کننده هستند و این یک واقعیّت است. با وجودی که سابقهٔ کار متعارف برای هر تولیدکنندهٔ نرم‌افزاری که در جستجوی کار بهتری است مهم است، امّا این تنها راه برای ارائهٔ اطلاعات به یک کارفرمای بالقوّه و احتمالی نیست.

شما باید اطلاعات سابقهٔ کاری خود را به‌صورت برخط نیز عرضه کنید. شما باید در لینکداین شرح حال[4] داشته باشید و اطلاعات سابقهٔ کارتان را

3- buzzwords

4- profile

جدول ۱۷-۱: راهنمایی‌هایی برای بهبود سابقهٔ کاری

راهنمایی	مزایا
سابقهٔ کارتان را روی اینترنت بگذارید	کارفرما راحت‌تر می‌تواند به آن دستیابی کند و این کار اگر به دنبال کار برنامه‌نویسی وب هستید، اهمیت دارد جلب توجّه کسی که سابقهٔ کاری را بررسی می‌کند
سابقهٔ کارتان را به شکل یگانه‌ای ارائه کنید	سابقهٔ کاری شما باید نشان دهد که چه کارهایی کرده‌اید و چه نتایجی به بار آورده است. این به خواننده نه تنها نشان می‌دهد که شما چه کارهایی می‌توانید بکنید، بلکه نشان می‌دهد که چه نتایجی توانسته‌اید به‌دست آورید و آن‌ها به طریق مشابه با استخدام شما به چه مزایایی ممکن است دست یابند
از زبان عمل- نتیجه استفاده کنید	
غلط‌گیری و ویرایش	حتی اگر یک سابقهٔ کاری‌نویس حرفه‌ای را به خدمت گرفته باشید، مطمئن شوید سابقهٔ کارتان کاملاً غلط‌گیری و ویرایش شده باشد. غلط تایپی و املایی نشانگر بی‌دقتی شماست

در آن قرار دهید و نیز باید نسخهٔ برخط سابقهٔ کارتان را هم داشته باشید تا بتوانید پیوند[5] آن را برای هر کس که خواستید بفرستید. تقاضا برای برنامه‌نویسی تحت وب بدون داشتن نسخهٔ برخط سابقهٔ کاری، مانند این است که یک نجّار حرفه‌ای ابزار کار برای خودش نداشته باشد.

قالب سابقهٔ کار هم باید مورد تجدید نظر قرار گیرد. سعی کنید کار منحصر به فرد و یگانه‌ای در تهیهٔ سابقهٔ کاری خود بکنید و به شیوه‌ای آن را ارائه کنید که توجّه خواننده را جلب کند. شما می‌توانید یا از شرکت‌های سابقهٔ کاری‌نویسی بخواهید که این کار را برایتان انجام دهند و یا سابقهٔ کارتان را از آن‌ها بگیرید و آن را به یک طراح گرافیک بدهید تا جذّاب‌ترش کند. من یکبار سابقهٔ کار یک برنامه‌نویس بازی‌های تصویری را دیدم که نسخهٔ برخط سابقهٔ کارش را به صورت یک بازی تصویری واقعی درست کرده بود (http://simpleprogrammer.com/ss-interactiveresume).

مطمئن هستم که زمان زیادی منتظر پیداکردن کار نمانده است. فهرستی از سابقهٔ کارهای خلّاقانه و جذّاب را که می‌توانند الهام‌بخش شما باشند در این نشانی ببینید:

http://simpleprogrammer.com/ss-beautiful-resumes

شما لزومی ندارد که زیباترین و جذّاب‌ترین سابقهٔ کاری را داشته باشید، امّا برای یک تولیدکنندهٔ نرم‌افزار مهم است که سابقهٔ کارش حرفه‌ای به نظر آید. اگر فکر می‌کنید که همان سابقهٔ کاری قدیمی که ده سال پیش با نرم‌افزار وُرد نوشته بودید و پر بود از غلط‌های تایپی و جملات بدساخت و تکراری، کارتان را راه می‌اندازد، در اشتباهید. اگر در جستجوی یک کار جدید هستید، یکی از بهترین سرمایه‌گذاری‌هایی که می‌توانید بکنید، درست کردن یک سابقهٔ کاری حرفه‌ای است.

اگر نخواهید یک فرد حرفه‌ای را به خدمت بگیرید چه؟

می‌توانم درک کنم که هنوز ترجیح می‌دهید خودتان سابقهٔ کارتان را بنویسید. شاید هزینه‌اش برایتان سنگین باشد یا این که حس می‌کنید کاری است که باید خودتان انجامش دهید.

اگر تصمیم گرفتید که خودتان سابقهٔ کارتان را بنویسید، برخی راهنمایی‌ها در جدول ۱۷-۱ آمده است که می‌تواند کمکتان کند.

5- link

اقدامات

• چه دنبال کار باشید یا نباشید، نسخه‌ای از سابقهٔ کارتان را برای برخی از کسانی که کار استخدام انجام می‌دهند بفرستید و نظرشان را دربارهٔ آن بپرسید. این افراد تعداد زیادی سابقهٔ کاری را می‌بینند و بهترین فرد برای این هستند که به شما بگویند سابقهٔ کارتان به اصلاح نیاز دارد یا نه.

• برخی از خدمات خلاصهٔ سوابق‌نویسی حرفه‌ای را مورد بررسی قرار دهید و نمونه‌های سابقهٔ کارهایی را که نوشته‌اند نگاه کنید. آن‌ها را چگونه با مال خود مقایسه می‌کنید؟

فصل ۱۸- بیش از حدّ شیفتهٔ فناوری نشوید

من نمی‌دانم شما آدمی مذهبی هستید یا نه. امّا مطمئنم که با من هم عقیده‌اید که بسیاری از جنگ‌های خونین و بی‌رحمانه در تاریخ، بر سر مذاهب و ادیان بوده‌اند.

من نمی‌گویم که باید دین را کنار گذاشت یا دین‌داری ذاتاً خوب یا بد است، امّا می‌خواهم شما را از این واقعیّت آگاه کنم که پیروی از اعتقادات جزمی و متعصّبانه می‌تواند بسیار فتنه‌انگیز و مخرّب باشد.

همین در مورد تولید نرم‌افزار هم صادق است. داشتن اعتقادات متعصّبانه دربارهٔ تولید نرم‌افزار و فناوری هم می‌تواند بسیار مخرّب باشد. با وجودی که ما کسی را به خاطر آن که iOS را بر اندروید ترجیح می‌دهد نمی‌کشیم، امّا بدمان نمی‌آید هنگامی که کسی نگاهمان نمی‌کند، با مشت ضربه‌ای به شکمش بزنیم.

من اعتقاد راسخ دارم که اگر شما در حرفه‌تان شیفتگی بیش از حدّ و وسواسی نسبت به فناوری نداشته باشید، پیشرفت بیشتری خواهید کرد. در این فصل، با هم این موضوع را بررسی خواهیم کرد.

همهٔ ما شیفتگی بیش از حدّ به فناوری داریم

این واقعیّت دارد. شما هم احتمالاً قبول دارید. شما به سوی برخی فناوری‌ها یا زبان‌های برنامه‌نویسی گرایش دارید و فکر می‌کنید که بهترین هستند. حداقل، اغلب برنامه‌نویسان این‌گونه‌اند. کاملاً طبیعی است، زیرا ما نسبت به آنچه انجام می‌دهیم شور و شوق داریم و هر جا که شور و شوق وجود داشته باشد، عقاید متعصّبانه و پرشور هم وجود خواهد داشت. نگاهی به ورزش‌های حرفه‌ای بیندازید.

مشکلی که با داشتن تعصّب و شیفتگی بیش از حدّ به فناوری وجود دارد این است که اغلب ما شیفتهٔ یک فناوری خاص هستیم زیرا آن فناوری، همانی است که ما با آن آشنا هستیم. این طبیعی است که اعتقاد داشته باشیم آنچه برگزیده‌ایم، بهترین گزینهٔ ممکن بوده است. در نتیجه، غالباً به هر پیشنهادی غیر از آن، کم‌محلی می‌کنیم. ما نمی‌توانیم با تمام فناوری‌های موجود آشنایی پیدا کنیم تا بهترین و آگاهانه‌ترین تصمیم را در بارهٔ این که کدامیک بهترین هستند بگیریم. بنابراین، تمایل داریم که همانی را که آشنایی داریم انتخاب کنیم و فرض کنیم که باید بهترین باشد- درغیر این‌صورت زندگی خیلی سخت می‌شود.

امّا این روند، با وجودی که طبیعی است، مخرّب و محدودکننده نیز هست.

هنگامی که ما متعصّبانه بر سر اعتقاداتی که فقط بر پایهٔ تجربیات خودمان است بایستیم، تمایل پیدا می‌کنیم که فقط با کسانی که همان اعتقاد را دارند هم‌نشـینی کنیم و از دیگران دوری کنیم. در آخر، در اجتماعاتی که فقط همان ایده‌ها بارها و بارها به گردش درمی‌آید، جدا می‌افتیم. به نقطه‌ای می‌رسیم که رشدمان متوقّف می‌شود زیرا تمام پاسخ‌ها را پیش از این یافته‌ایم.

من بخش زیـادی از زندگی حرفه‌ایـم را با اعتقـادات متعصّبانه دربارهٔ سیسـتم‌های عامل، زبان‌های برنامه‌نویسـی و حتی ویراستارهای متن[6] گذرانده‌ام تا آن که دانشم بیشتر شد و شروع به فهم این مطلب کردم که نبایـد فقط یک فناوری را به‌عنوان بهترین فناوری برمی‌گزیدم و بقیه را پایین‌تر و بدتر از آن در نظر می‌گرفتم.

همه چیز خوب است

همهٔ فناوری‌ها عالی نیستند، امّا اغلب آن‌هایی که مورد پذیرش گسترده‌ای قرار گرفته‌اند، دست‌کم «خوب» هستند. چیزی که دست‌کم خوب نباشد، مشکل بتواند موفّق شود و به‌طور گسترده‌ای معروف و مورد استفاده واقع گردد. البته، شرایط در طول زمان تغییر می‌کند، امّا درک این نکته اهمیّت دارد که دست‌کم در یک برههٔ تاریخی، تقریباً هر فناوری، خوب یا حتی عالی در نظر گرفته شده است.

داشتن یک دیدگاه به شما در درک این نکته کمک می‌کند که در بسیاری از موارد، تنها یک راه حل خوب یا برتر برای یک مسئله وجود ندارد. تنها یک زبان برنامه‌نویسی، چهارچوب[7]، سیستم عامل یا ویراستار متن خوب یا برتر وجود ندارد. ممکن است شما یک فناوری خاص را بیشتر از بقیه دوسـت داشته باشید و ممکن است کارایی شما در استفاده از یک زبان برنامه‌نویسی خاص بیشتر از بقیهٔ زبان‌ها باشد، امّا این دلیل نمی‌شود که آن فناوری یا آن زبان برنامه‌نویسی بهترین باشد.

تغییر عقیدهٔ من

من مدّت‌ها این اعتقاد را داشـتم. ساعت‌های طولانی بحث می‌کردم که چرا ویندوز خیلی بهتر از مَک اسـت. بارها دربارهٔ این که چرا C# و سایر زبان‌های نوع ایستا خیلی بهتر از زبان‌های پویا مانند پِرل و روبی هستند داد و فریاد راه می‌انداختم. حتی با شرمندگی باید بگویم که گاهی دیگر تولیدکنندگان نرم‌افزار را که عقیدهٔ دیگری داشـتند سرزنش می‌کردم. چطور جرئت می‌کردند به فناوری دیگری غیر از آنچه من اعتقاد داشتم، اعتقاد داشته باشند؟

تجربه‌ای که چشـم مرا باز کرد هنگامی بود که برای نخسـتین بار از من خواسته شد تا سرپرست تیمی برای انجام یک پروژهٔ جاوا بشوم. تا آن زمان، من اساسـاً یک برنامه‌نویس .NET. و متمرکز بر روی C# بودم. (راستش را بخواهم بگویم، پیش از آمدن .NET. تعصّب زیادی روی C++ داشتم.) من نمی‌توانستم ایدهٔ کارکردن با جاوا را هضم کنم. از نظرمن، جاوا در مقایسه با زیبایی C#، زبان کثیفی بود. وقتی بلد نبودم از عبارت‌های لاندا[8] استفاده کنم، چطور می‌توانستم از نوشتن کد جاوا لذّت ببرم؟

سـرانجام تصمیم گرفتم کـه آن کار را بپذیرم، زیرا فرصت خیلی خوبی برایم بود و من فکر کردم چون یک قرارداد کوتاه مدّت اسـت، می‌توانم برای یک سـال، کمی کمتر یا بیشـتر، آن را تحمّل کنم. امّا پذیرش آن کار، یکی از بهترین تصمیم‌های زندگی حرفه‌ایم از آب درآمد. کارکردن با فناوری‌ای که از آن نفرت داشتم، باعث شد تا از زاویهٔ متفاوتی به تمام فناوری‌ها نگاه کنم. به این نتیجه رسیدم که جاوا اصلاً زبان بدی نیست. و دریافتم که چرا بعضی از برنامه‌نویسان آن را بر C# ترجیح می‌دهند.

در طول چند سـالی که بر روی آن پروژهٔ جاوا کار کردم، خیلی بیشتر از تمـام دوران کاریم تا آن مقطع، چیز یاد گرفتم. به جای چند ابزاری که پیش از آن خودم را به استفاده از آن‌ها محدود کرده بودم، ناگهان جعبه ابزار بزرگی پر از ابزارهایی به‌دسـت آوردم که می‌توانستم به کمک آن‌ها برای حل هر مسئله‌ای اقدام کنم.

از آن نقطه به بعد، همان طرز فکر بازی را که نسـبت به جاوا پیدا کرده بودم به سـایر زبان‌های برنامه‌نویسـی هم تعمیـم دادم، حتی زبان‌های پویا، و توانسـتم با اسـتفاده از چیزهایی که از هر یک از آن‌ها یاد گرفته بودم، برنامه‌نویس بهتری در همهٔ آن‌ها شوم. من در مورد عقایدم دربارهٔ سیسـتم‌های عامل و چهارچوب‌ها نیز عقب‌نشینی کردم و پذیرفتم که پیش از داوری دربارهٔ هر چیز، باید آن را امتحان کرد. من اگر این تجربه را به‌دست نمی‌آوردم، احتمالاً به نوشتن این کتاب هم نمی‌پرداختم و به جای آن، مثلاً کتابی می‌نوشـتم با عنوان «چرا C# بهترین زبان است و بقیهٔ زبان‌ها خیلی بد هستند.»

گزینه‌های خود را محدود نکنید

نکتهٔ اصلـی در اینجا این اسـت که گزینه‌های خـود را محدود نکنید. پافشـاری پرشـور و حرارت در مورد این که فناوری مورد گزینش شما بهترین اسـت، به قیمت نادیده گرفتن و کوچک‌شمردن بقیهٔ فناوری‌ها، کار درستی نیست. ایستادگی بر سر این دیدگاه، فقط باعث آسیب دیدن خود شما خواهد شد.

از سوی دیگر، اگر ذهنیّت بازی نسبت به فناوری به‌طور کلّی، و نه فقط آن فناوری که با آن آشنا هستید، داشته باشید، فرصت‌های بسیار بیشتری برایتان به‌وجود خواهد آمد.

اقدامات

- فهرسـتی از تمام فناوری‌های مـورد علاقه‌تان یا فناوری‌هایی که فکر می‌کنید برتر از بقیه هستند، تهیه کنید.
- برای هر عنصر آن فهرسـت، فکر کنید که چرا به سـوی آن فناوری کشیده شده‌اید و از چه معیاری برای توجیه آن استفاده کرده‌اید. آیا تجربهٔ عملی از به‌کارگیری رقیبان آن فناوری دارید؟
- یکی از فناوری‌هایی را که بدتان می‌آید انتخاب کنید و یک نفر را که عاشـق آن است پیدا کنید. سؤالات صادقانه‌ای از او دربارهٔ این که چرا به آن فناوری خاص علاقه‌مند است بپرسید. سپس تلاش کنید که خودتان هم از آن استفاده کنید.

ادامه دارد...

6- text editor
7- framework
8- Lambda expression

تحول دیجیتال به زبان ساده

(قسمت دوم)

بتول ذاکری

پست الکترونیکی: Bzakeri2010@gmail.com

مقدمه مترجم

ایــن روزها همه جا بحث از تحول دیجیتال یا شــاخه‌های آن ماننــد اقتصاد دیجتیال، بانکداری دیجیتال، دولــت دیجیتال، فناوری‌های دیجیتال، نقشــه راه دیجیتال، روندهای رشــد و پیشــرفت تحول دیجیتال و... اســت. و این واژگان، مفاهیم و روندها روز به روز فراگیرتر می‌شود. اما علیرغم این فراگیری هنوز مفاهیم پایه و مولفه‌های اصلی و چگونگی برخورد با آن برای سازمان‌ها و موسسات و مدیران آن‌ها روشــن نیســت. کتاب حاضر:Digital transformation for dummies تالیف آقایان Kerravala Zeus و Lawrence Miller که من آن را «تحول دیجیتال به زبان ساده» ترجمه کرده‌ام، از مجموعه انتشارات موسسه Wiley & Sons, Inc. John است که به زبانی ساده ضرورت همگام شــدن با تحول دیجیتال، فرصت‌های حاصل از تحول دیجیتال، مولفه‌های تحول دیجیتال، اســتراتژی رویارویی با تحول دیجیتال، فناوری‌های دیجیتال، تجربه مشتری دیجیتال، کارکنان و محیط کار دیجیتالی و مشخصه‌های یک شرکت یا سازمان دیجیتالی را تشریح می‌کند. در این شماره فصول ۳ و ۴ و ۵ کتاب ارائه شده است.

فصل سوم- ارائه «تجربه مشتری» دیجیتالی برتر

در این فصل شما تجربه مشتری دیجیتال و معنی آن را برای سازمان خود کشف می‌کنید.

دیجیتالی شدن تجربه مشتری را بازتعریف می‌کند

تجربــه مشــتری در محیط فوق رقابتی امروز یک عامل تمایز اســت. بیش از هر زمانی دیگر تجربه مشــتری از طریق تعامل‌های دیجیتالی شکل گرفته و ارائه می‌شود.

در حالــی که هنوز اکثــر ارتباطات مشــتریان، مبتنی بر صداســت، مشتریان امروز بیشــتر بر روش‌های دیجیتالی مانند ایمیل، پیام‌های متنی، گفتگو در وب، و رســانه‌های اجتماعی متکی هســتند. فارستر اظهار می‌دارد اســتفاده از گزینه‌های سلف‌سرویس در سال ۲۰۱۴ تا ۷۶٪ افزایش یافت، در حالی که ۵۸٪ مصرف‌کنندگان گزینه‌های گپ برخــط را انتخاب کردند و ۳۸٪ پیغام‌های متنی و ۳۷٪ از تعامل‌های توئیتری استفاده کرده‌اند.

مصرف کنندگان از طریق ابزار منتخب خود، هرجا که هستند، انتظار انعطــاف پذیری در تعامل‌ها را دارند. انتظار دارند که بتوانند در حین حرکت بین رسانه‌های مختلف حرکت کنند.

اووم گــزارش می‌دهد کــه ۷۴٪ مصرف‌کنندگان امروز وقتی به دنبال مراقبت‌های مشتریان می‌گردند، حداقل از سه کانال یا بیشتر استفاده می‌کنند.

در عیــن حــال مصرف‌کنندگان تقویت شــده به‌وســیلهٔ رســانه‌های اجتماعــی، به‌صورتی فعّالانه نظرات و پیشــنهادهای خود را در مورد تجاربشان به رسانه‌های اجتماعی، وبگاه‌ها و انجمن‌ها می‌فرستند. در این محیط داستان یا فیلم یک تجربه مثبت یا منفی مشتری می‌تواند با زدن یک کلیک ماوس همه جا پخش شود.

بنابراین تجربه مشـتری به یک میدان جنگ جدید برای تمایز رقابتی در این عصر دیجیتالی تبدیل شده است.

• یک مطالعـه اخیر از کمپانـی Walker Information پیش‌بینی می‌کند که تا سال ۲۰۲۰ تجربه مشتری به‌عنوان متمایزکننده نشان تجاری از قیمت و محصول سبقت خواهد گرفت

• گارتنـر در یکـی از مطالعات اخیر خود به اهمیت تجربه مشـتری تاکید دارد. و این مطالعه نشان می‌دهد که ۸۹٪ شرکت‌ها امروز اساسا برمبنای تجربه مشتری رقابت می‌کنند، برخلاف فقط ۴ سال گذشته که این نرخ ۳۶٪ بوده است.

• تحقیق انجام شـده توسط LivePerson نشان می‌دهد که ۸۲٪ از مصرف‌کنندگان می‌گویند برطرف کردن سـریع مشکل، عامل شماره یک است که منجر به خدمات عالی می‌شود.

• SLD گـزارش می‌دهد که ۶۴٪ از مصرف‌کنندگان بعد از شکسـت عمده در تجربه مشـتری و نشـان تجاری، رقیـب را ترک می‌کنند و نشـان‌های تجاری متوسـط ۶۵٪ درآمد خود را برای هرتجربه منفی مشتری از دست می‌دهند.

پس اگر کسـب‌وکاری نتواند تجربه مناسب و صمیمی که مشتری به دنبال آن است را فراهم کند، رقیب او خواهد توانست.

بنابرایـن، ارائه رضایت بخش تجربه مشـتری یـک اولویت بالا برای هرکسـب‌وکاری خواهـد بود. متاسـفانه خلق و مدیریـت این تجربه هیچگاه به این اندازه پیچیده نبوده است. علاوه بر آن رکود اقتصادی و فضـای بـازار در حال تکامـل، کاهش فزاینده هزینه‌هـا، و افزایش کارایی عملیاتی را برای هرکسب‌وکاری حیاتی ساخته است.

با تغییر ارائه تجربه مشـتری دیجیتالی از وضعیت «خوب اسـت که داشته باشیم» به یک سرویس ضروری، هرکسب‌وکاری که با مشتریان خـود تعامل دارد، باید از فناوری‌های مناسـب بـرای ارائه تجربه ای مداوم از طریق تمام رسـانه‌ها برخوردار و همچنین راهبرد مشخصی برای گسترش دامنه این خدمات داشته باشد.

تحـول دیجیتال باید به یـک اقدام با اولویت بالا برای کسـب‌وکارها تبدیل شـود و با بازتعریف تجربه مشتری آغاز کنند. سازمان‌هایی که این را درک کنند و بتوانند تجربه مشتری دیجیتال برتری ارائه کنند، شکوفا شـده و راهبر صنعت خود خواهند شـد. وکسب‌وکارهایی که نتوانند، برای رقابتی ماندن باید تلاش زیادی کنند.

متصل ماندن به مصرف‌کنندگان امروز تلفن همراه

تا همین اواخر صدا در مقایسـه با سایر روش‌های سنتی مانند نامه یا بازدید شخصی، سـریع‌ترین و مناسب‌ترین روش تعامل با کسب‌وکار بود. در حالی که امروز دیگر این‌طور نیست. علیرغم فراگیر شدن تلفن همراه، امروزه استفاده‌کنندگان با در دسترس داشتن مجموعه‌ای غنی از راه‌حل‌های فناورانه، برای تماس با کسـب‌وکار هر روز کمتر و کمتر از صدا اسـتفاده می‌کنند (حتی با یکدیگـر). مطالعه‌ای از Nielsen در ۲۰۱۴ نشـان می‌داد که در ایـالات متحده آمریکا تماس صوتی با تلفن‌های هوشمند، به زحمت به سه درصد می‌رسید. و این‌که بیشتر اسـتفاده از طریق پیام متنی، رسـانه‌های اجتماعی و سایر کاربردها بوده است.

تاثیر این تغییر الگوی استفاده در کسب‌وکارها مشخص است. درست همانـنـد تماس‌هـای صوتی که زمـان انتظار همراه با ارسـال نامه و ناراحتی‌های همراه با ملاقات‌های فیزیکی از یک کسـب‌وکار را حذف کـرد، گزینه‌های ارتباطات دیجیتال هـم، زمان انتظار را کاهش داده و نیـاز به اتصال زنده صوتی با مرکز خدمات مشـتری را حذف کرده است. وب‌گپ‌ها، و پیام‌های متنی راه‌حل‌هایی مناسب با هر وضعیت را ارائه می‌کنند. این راه‌حل‌ها زمان انتظار را حذف کرده و رضایت فوری از این‌که مسـئله به سرعت برطرف شده است را موجب می‌شود و به مشتری امکان انجام چند کار در حین انتظار را می‌دهد.

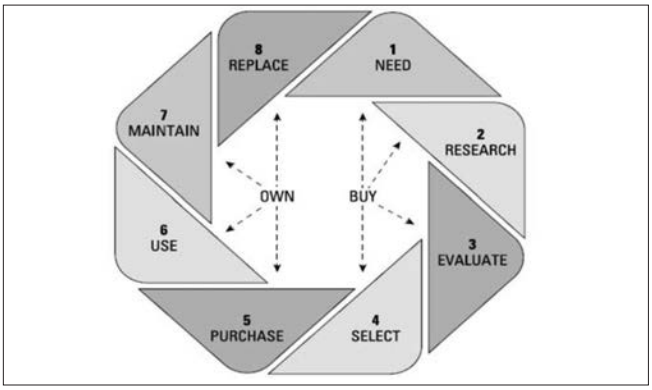
در این دنیای همیشـه برخط، همیشه متصل، دنیای همواره در حال پخش، انتظارات مشـتریان تغییر کرده اسـت. مصرف‌کنندگان امروز دیگر راضی به کارکردن در سـاعات تعیین شده کاری نیستند. انتظار دارند در هرزمانی شب یا روز بتوانند متصل شوند. انتظار دارند که خود انتخـاب کنند که چگونه به کانال‌های ارتباطی وصل شـوند و انتظار دارند که پاسـخ‌های فوری به جسـتجوهای خود از طریق تعامل‌های یکپارچه دیجیتال دریافت کنند. همان‌طور که گارتنر اشـاره می‌کند، شکسـت در پاسـخ به کانال‌های اجتماعی منجربه ۱۵٪ افزایش نرخ چانه زنی برای مشتریان موجود می‌شود.

درک چرخه زیست مشتری

ارائه تجربه برتر مشـتری ابتدا مستلزم درک مشکلاتی است که مشتری با آن روبروست. با اکثر خدمات، مشتری به نقطه ادغام برای چندین ارائه دهنده خدمت در سراسر چرخه زیست مشتری در می‌آید (شکل ۳-۱)

اگر مشـتری به چند خدمت نیاز داشته باشـد باید به دنبال چندین ارائه دهنده خدمت بگردد تا نیازهایش تامین شود. مثلا در بانکداری، مشتری ممکن است به دنبال چندین بانک بگردد تا نیازهای مختلفی مانند چک، برنامه بازنشسـتگی، رهن، وام خرید خودرو و سایر نیازها را بـرآورده کنـد. حتی اگر یک موسسـه واحد تمام ایـن خدمات را عرضه کند، مشتری برای هریک از آن‌ها با واحدهای مختلف سازمانی مسـتقل باید روبرو شـود. یک تجربه مشـتری برتر به مشتریان خود دسترسـی یکپارچه به کلیه خدمات مـورد نیاز در یک مکان واحد را می‌دهد.

مصرف‌کنندگان می‌خواهند کانال و ابزار مورد نظر خود را برای برقراری ارتباط با ارائه دهندگان خدمت، و هر وقت نیاز دارند، اسـتفاده کنند، این می‌تواند یک تماس تلفنی با موبایل قبل از ترک خانه، ارسال یک پیغام متنی وقتی در قطار هستند و مشارکت در یک جلسه ویدیویی در اداره باشـد. بنابراین خیلی مهم است که کسـب‌وکارها راهبردی یکپارچه برای تعامل با مشـتریان داشـته باشـند که به آن‌ها کمک کند در صدر ذهن مشـتری قرارگیرند و لحظه صفر حقیقت جایی که



شکل۳-۱: چرخه زیست مشتری

مشـــتری تصمیم‌گیری می‌کند که چه کالایی بخرد یا از چه خدماتی استفاده کند را ضبط کنند.

توسعه راهبرد تجربه مشتری

رقابـــت در عصر دیجیتال به‌طور فزاینده ای دشـــوار می‌شـــود. فناوری سریع‌تر از همیشه پیشرفت می‌کند، و شرکت‌ها باید به چالش‌های بازار از رقبای سنتی خود –تا رقبای بومی دیجیتال- بپردازند.

حقیقت این اســـت که هیچ صنعتی مصون نیســـت. دیجیتالی‌شـــدن هرصنعتی را متحول و چشـــم‌انداز رقابت را به ســـرعت تغییر می‌دهد. بزرگ‌ترین پرسش برای کســـب‌وکارهای امروز این است که چگونه در این عرصه به‌طور فزاینده شلوغ، متمایز شوند.

از نظر تاریخی کسب‌وکارها بر راهبری محصول یا داشتن کمترین قیمت رقابت می‌کردند، اما این رویکرد بیش از این پایدار نیســـت. محصولات با کیفیت امروز در بالای جدول هستند و نگهداشتن پایین‌ترین قیمت یعنی حاشـــیه سود نازک و مشکل‌تر ساختن نوآوری به منظور پایداری رهبر بازار ماندن

توســـعه یک راهبرد متمرکز بر ارائه تجربه مشـــتری برتر مســـتلزم آن است که کســـب‌وکارها در مورد این‌که چگونه با مشتری تعامل داشته باشـــند، طور دیگری بیندیشند. تمرکز آن‌ها باید از انجام تراکنش‌های فـــردی به ایجاد روابـــط طولانی و پایـــدار و قابل اعتماد کـــه می‌تواند تمام جنبه‌های چرخه زیســـت مشـــتری را درخود جـــای دهد، تغییر کند.

نکات کلیدی در مورد ساخت تجربه مشتری برتر که بتواند بر فرصت‌های خلق شده در عصر دیجیتال سرمایه‌گذاری کند، شامل موارد زیر است:

• ساخت تجربه تماس یکپارچه[1]

مفهوم تماس یکپارچه به‌صورتی گسترده پذیرفته شده، و کسب‌وکارها را قادر می‌ســـازد که با مشتری از طریق هرکانالی از جمله ویدیو، صدا، پیغام متنی، گپ، یا ســـایر صحبـــت کنند. تماس یکپارچه با روش‌های سنتی تعامل‌ها متفاوت است، زیرا ارتباطات در سرتاسر کانال‌ها به‌طور کامل یکپارچه است. مثلا اگر خرده فروشی ارتباطات تماس یکپارچه را اجرا کند، یک نماینده در داخل فروشـــگاه می‌تواند به سادگی به همان اطلاعات تاریخی دسترسی داشته باشد که از یک نفر روی خط می‌توان پرسید.

• پشتیبانی محدوده کامل کانال‌های دیجیتالی

صرف‌نظر از این‌که کانال ارتباطی، یک رسانه اجتماعی، گپ‌وبی، ایمیل یا پیغام متنی باشـــد، همه کانال‌ها نماینده نوعی سطح اهمیت کانال‌ها برای مشـــتریان شماســـت. اگر برای به‌کارگیری تمام گزینه‌ها آمادگی ندارید، حداقل باید کانال‌هایی که بیشترین اهمیت برای کسب‌وکار شما دارند را براســـاس اطلاعات دموگرافیک و طبیعت ارتباطتان با مشتری شناســـایی کنید. و رویکردی پیمانه‌ای را که قابلیت اندازه‌پذیری داشته باشد و بخصوص بتوانید در طول زمان قابلیت‌های خاصی را هرجا لازم باشد به آن وصل کنید به‌کار بندید.

• ایجاد تجربه مشتری پیشرفته

صرف‌نظر از این‌که مشتری کدام کانال را برای استفاده انتخاب می‌کند، سازمانها باید اطمینان حاصل کنند که تجربه موجود مشتری را خشنود میکند، و این شـــامل توسعه بهترین تجربه‌ها از طریق رابط‌های مبتنی بر وب و موبایل خواهد بود.

• پیش‌بینی رفتار

در محیط کسب‌وکار رقابتی امروز، شناخت بهتر مشتریان نسبت به قبل حیاتی است. کسب‌وکارها باید چندین نوع داده مختلف، شامل اطلاعات اجتماعـــی و رفتار خرید مشـــتری را جمع آوری کـــرده و آن‌ها را برای پیش‌بینی این‌که مشتری چه خواهد خواست، تحلیل کنند.

• خودکار کردن جستجوهای رایج با قابلیت‌های خود سرویس دهنده با ابزارهای پیشـــرفته تجربه مشتری، خودسرویس دهندگی دیگر فقط به تعامل‌های مبتنی بر صدا محدود نمی‌شـــود. پرســـش‌های متداول، تراکنش‌های ســـاده از طریق صدا، گپ وبی، یا پیغام‌های متنی هرکدام که باشـــد، و پاسخ‌های نظرسنجی مشـــتریان را برای تصمیم‌گیری در مورد این‌که کدام فرایندها برای الکترونیکی شـــدن مناسب‌تر هستند، تحلیل کنید. از قابلیت‌های روال‌مند گردش کار دیجیتالی برای فراهم کردن سلف سرویس برای مشتریان از طریق ایمیل، تاییدهای خودکار، پاسخگوی خودکار، گپ وبی، و حتی جستجوهای مربوط به پیغام‌های متنی ورودی و خروجی استفاده کنید.

گزینه‌های سلف ســـرویس فرصت‌های قابل توجهی برای بهبود تجربه مشـــتری و کاهش هزینه‌ها ارائه می‌کنند، امـــا تضمینی برای موفقیت نیست. مثال‌های فراوانی از سازمان‌هایی وجود دارد که به اندازه کافی با ناامیدی‌های مشتریان در مورد خودکارسازی همدردی نمی‌کنند، و در نتیجه گزینه‌های سلف سرویسی ایجاد می‌کنند که انتظارت مشتریان را برآورده نمی‌کنند.

فصل۴ – ایجاد راهبرد دیجیتال

تبدیل شدن به یک کسب‌وکار دیجیتال، باید برای کسب‌وکار و رهبران فنـــاوری اطلاعات یک برنامه و اقدام با اولویت بالا باشـــد. در بســـیاری

1- omnichannel

سازمان‌ها هیئت مدیره سازمان- مسئول موفقیت بلند مدت یک کسب‌وکار- اقدامات دیجیتال را برای خلق یک بنیاد چابک که شرکت را قادر می‌سازد به سرعت با روندهای سریع تکاملی کسب‌وکار سازگار شود، هدایت می‌کند

وقتی صحبت از تحول دیجیتال می‌شود، دکمه آسانی برای فشار دادن وجود ندارد، اما این فصل چگونگی ایجاد یک راهبرد دیجیتال برای سازمان شما را تشریح می‌کند.

توسعه قابلیت‌های بنیادی در سازمان‌های دیجیتالی

از آنجا که پتانسیل فناوری‌های کسب‌وکار دیجیتال برای ایجاد تحول بسیار زیاد است، کسب‌وکارها در تمام صنایع باید به تاثیرات احتمالی فناوری‌های کسب‌وکار دیجیتال برای ایجاد اختلال در بسیاری راه‌های سنتی انجام کسب‌وکارشان بپردازند. اگر کسب‌وکارها نتوانند با تغییر همگام شوند، ممکن است مجبور به وضعیت تلاش برای زنده ماندن یا به‌طورکل از بین رفتن شوند.

برای اطمینان از مرتبط بودن کسب‌وکار و فعال کردن نوآوری مداوم شرکت‌ها برای این‌که پیشرفت کنند، باید یک راهبرد دیجیتال را توسعه دهند که:

• فرایندها و مدل‌های کسب‌وکار را متحول کند.

تحول فرایندهای کسب‌وکار زمان رسیدن محصول به بازار و عملیات ناب‌تر که باعث موفقیت سازمان‌ها در محیط رقابتی امروز می‌شود را سریع‌تر می‌کند. برطبق نظر SCM World چرخه زمانی معرفی یک محصول جدید در کارخانجات با فرایندهای دیجیتال ۲۳٪ کاهش می‌یابد.

• تجربه کاربر را شخصی سازی کند.

انجام این کار می‌تواند منجر به افزایش وفاداری مشتری و بینش بهتر برای فعال کردن مدل‌های کسب‌وکاری قابل پیش‌بینی شود. یک نظرسنجی از Accenture در سال ۲۰۱۳ نشان می‌داد که ۶۶٪ از مصرف‌کنندگان/ مشتریان، تامین کنندگان خود را به‌خاطر تجربه مشتری تغییر دادند. ما به سرعت به عصری وارد می‌شویم که تجربه مشتری مهم‌ترین عامل تمایز رقابتی برای کسب‌وکار ها در تمام صنایع است.

• نیروی کار را تقویت کند.

نیروی کار تقویت شده، نیروی «درگیر کار کامل» خواهد بود. یک نظرسنجی اخیر گالوپ نشان می‌دهد که ۸۷٪ کارکنان در دنیا «غیر درگیر» در کارند. پایین آوردن این نرخ منجر به بهره وری بالاتر و نگهداری کارکنان می‌شود.

آغاز سفر تحول دیجیتال

تحول دیجیتالی کسب‌وکار نمی‌تواند یک «برنامه و ابتکار حوزه فناوری اطلاعات» باشد. برای موفقیت، کسب‌وکار و فناوری اطلاعات باید با هم کار کنند. برای خلق محیطی که در آن کارکنان بتوانند تحول دیجیتال را در سازمان خود هدایت کنند. برای دیجیتالی شدن یک سازمان اقدامات زیر باید انجام شود:

• تعیین نتایج کسب‌وکاری که باید به آن دست یافت

نتایج خاص مورد انتظار مانند بهبود تجربه مشتری، تجربه نیروی کار، کارایی فرایندها و عملیات کسب‌وکار را انتخاب کنید

• ایجاد فرهنگ «اول دیجیتال»

این باید از سطح مدیران ارشد آغاز شده و به کل سازمان تسری داده شود.

• اتصال هرچیزی که به نتایج مربوط می‌شود و جمع آوری اطلاعات در مورد آن‌ها

یک شرکت دیجیتالی بیش از حد توزیع شده است. هربخش آن به زنجیره ارزش متصل شده است و از هرنقطه اتصال به‌عنوان یک منبع داده برای جمع آوری داده‌های دقیق و عمیق استفاده می‌شود.

• الکترونیکی کردن فرایندها تا سرحد امکان

یک سازمان دیجیتالی می‌تواند به‌طور نمایی نسبت به یک سازمان سنتی پیچیده‌تر باشد. کاربرد موثر فناوری‌های دیجیتال نیازمند خودکارسازی حتی الامکان فرایندها در سرتاسر سازمان است.

• تحلیل داده‌ها و کسب بینش جدید

کسب‌وکارهای دیجیتال ثروتی از داده‌ها در دسترس دارند؛ مزیت‌های رقابتی دراز مدت از طریق مهار مستمر داده‌ها، تحلیل آن‌ها، کسب بینش جدید و سازگاری سریع و فعالانه با روندهای مهم بازار و مشتری ایجاد می‌شود.

با یک راهبرد دیجیتال موثر، مشتریان، کارکنان و کسب‌وکار می‌توانند مزایای زیر را به‌دست آورند:

• مشتریان

□ مشتریان تقویت شده با گزینه‌های انعطاف پذیر ارتباطی برای استفاده هرجا مناسب باشد

□ گزینه‌های هوشمند، یکپارچه سلف سرویس خودکار و در دسترس به‌صورت ۷/۲۴

□ نیازهای برآورده شده از طریق مهارت‌ها با ارجاع به نمایندگان ترجیح داده شده

□ جستجوهای خیلی سریع پاسخ داده شده ازطریق تعامل‌های سریع برمبنای تمام دانش سازمان

• کارکنان

□ دستاوردهای فوری و طولانی مدت در کارایی، حذف دوباره‌کاری‌ها و تلاش برای بهبود بهره‌وری

□ رضایت شغلی بالاتر و ریزش کمتر پرسنل از طریق دانش انباشته آزاد شده

□ کارکردن سریع‌تر از خانه یا از راه دور با فرایندهای همسو شده با ابزارهای ارتباطات

• کسب‌وکار

□ اهرم عادات مشتری دیجیتال و اشتها به کانال‌های جدید ارتباطی، در حالی که از کاهش قابل توجه هزینه‌ها در هرتعامل سود می‌برد

□ بهبـود صرفه‌جویی اقتصـادی چون عاملان چنـد وظیفه‌ای به‌طور همزمان با ارتباطات چندگانه برخورد می‌کنند.
□ لذت بردن از افزایش مزیت های رقابتی از طریق ارائه سـطوح عالی خدمات
□ جلوتـر از منحنی ترجیحات ارتباطاتی مشـتری قرار گرفتن، مانند پیشرفت مداوم کاربردهای تلفن همراه
□ دریافـت بازگشـت سـرمایه با داشـبرد لحظه‌ای (زمـان واقعی) از سنجه‌های جامع و دقیق تجربه مشتری و شاخص‌های کلیدی عملکرد.
□ انطبـاق داده‌ها با هزینه مقرون به‌صرفه، قابل پیش‌بینی و برمبنایی قابل اندازه‌گیری و سازگار در سرتاسر کانال‌های ارتباطی
□ پذیـرش تغییر با یک بُن‌سـازهٔ[2] انعطاف‌پذیر قابل اثبات درآینده که مشتری را کاملا به مشارکت وا می‌دارد، و آماده پاسخگویی و پرداختن به تکامل ترجیحات مشتری است

۷ گام برای خلق تجربه مشتری دیجیتالی

برای انتقال از وضعیت فعلی به وضعیت دیجیتال گام‌های زیر را بردارید:
۱- مسئولیت به عهده بگیرید
تعیین کنید که در نهایت چه کسـی مسـئول مشارکت مشتری است، مثـلا مدیرعامل، مدیر فروش یا بازاریابی، یا مدیر خدمات مشـتریان- سپس راهبرد تجربه مشتری را تعریف کنید
۲- سودبران را شناسایی و درک کنید
تا حد ممکن در مورد تجارب نمایندگان خدمات مشتریان و ترجیحات مشـتری خود اطلاعات کسـب کرده، سپس اطمینان حاصل کنید که مشتری به‌صورتی بهینه با جریان کارها همسو ست.
۳- جستجوهای رایج را با قابلیت‌های سلف سرویس خودکارکنید
با استفاده از ابزارهای مدرن تجربه مشتریان، سلف سرویس امروز دیگر فقط به صدا محدود نمی‌شود. سـوالات رایج، تراکنش‌های نمایندگان و پاسـخ نظر سنجی‌های مشـتریان را تحلیل کنید تا معلوم شود چه فرایندهایی باید خودکار شوند.
۴- برای دامنه کامل کانال‌های دیجیتال آماده شوید
کانال‌های دیجیتال را خواه رسـانه اجتماعی باشـد یا گپ وبی، ایمیل باشد یا متن،یا همه این‌ها، مشخص کنید کدام یک برای مشتریان شما مهم‌تر است. و از یک رویکرد ماژولار که به شما امکان می‌دهد به مرور زمان آن را ارتقاء و گسترش دهید، به‌کار ببرید. و قابلیت‌های خاص را هرجا امکان پذیر باشد، به کانال‌ها وصل کنید.
۵- نمایندگان خود را تقویت کنید
جدیدترین ابزار مدرن که کارکنان شما را قادر سازد موثرتر و با انعطاف بیشتر کار کنند را به‌کار ببرید
۶- یک کشتی مطمئن را برانید
محیطی مدرن و قابل اطمینان خدمات مشـتریان بسـازید که توزیع تماس خودکار را با گردش کار فرایندهای دیجیتال و صدا و نقاط تماس چندگانه مشتری یکپارچه می کند.

۷- سنجه‌های مدیریتی و گزارش‌دهی موثر به‌کار بگیرید.
با استفاده از ابزار با ویژگی‌های زمان واقعی و غنی مدیریت و گزارشدهی، قابلیت دید عملیاتی ومداوم کسب‌وکاری ایجاد و نگهداری کنید.

فصـل۵ – ارتباطـات و همکاری‌هـای یکپارچـه[3] در سازمان دیجیتال

در دنیای ارتباطات و همکاری‌های یکپارچه، سازمان دیجیتالی متصل، زمینه کاملی از فرایندهای کسـب‌وکار با ارتباطات روان و طبیعی دارد که به‌صورتی یکپارچه در کل فضای کاری و تجربه مشتری جاری است. در این فصل می‌بینید که چگونه راه‌حل‌های UCC کسب‌وکار دیجیتالی را متحول می‌کند.

کسب‌وکار دیجیتالی به ارتباطات زمان واقعی[4] نیاز دارد

کارکنـان از اطلاعات و تحلیل‌هایی کـه برای ارتباطات اهمیت دارد، با هدف حذف زوایـد، کارآمدترکردن کار، به‌کارگیـری همه جانبه توان شرکت برای هرمشارکت مشتری استفاده می‌کنند.
سـازمان دیجیتالی می‌تواند بـه میزان زیادی اطلاعـات (متنی) را به ارتباطات و تصمیم‌گیری بکشاند. در حالی که تمام این اطلاعات توسط مدیریت ارتباط با مشـتریان و سـایر کاربردها ثبت می‌شود، کارکنان شـرکت با در دست داشـتن این دانش زمینه‌ای می‌توانند به مشتریان خود رسیدگی کنند. از طریق یک چارچوب واحد که بر مبنای محتوای کاربردهای کسب‌وکاری شکل گرفته و دربرگیرنده موبایل، اداره و ابزار ارتباطی کسب‌وکار است، کارکنان می‌توانند با مشتریان در زمان واقعی تعامل برقرارکنند. این چارچوب به سادگی قابل استفاده در اختیار همه کارکنان از خدمات گرفته تا کارکنان پشتیبانی در اداره قرار می‌گیرد.
سـازمان دیجیتـال ارزش کسـب‌وکاری قوی به بـازار عرضه می‌کند. سازمانی با این قابلیت می‌تواند زمان روبرو شدن کارمند با هر مشتری را صرفه‌جویی کند، با مشـعوف کردن مشـتری، رضایت بالاتری ایجاد کنند و بهره وری بیشتری از طریق کار افزایشی یا تقاضای اضافی بازار حاصل نمایند.
کارکنان در سازمان دیجیتالی، دیگر وقت زیادی صرف آماده‌سازی برای گفتگو با مشـتریان نمی‌کنند، بلکه آن‌ها غرق در پیغام‌های مشـتریان هسـتند و با درگیر کردن مشـتری کار تجاری می‌کننـد. کارکنان در سازمان‌های دیجیتالی از داشتن قابلیت‌هایی که عمدتا موبایل هستند، مشعوفند. درحالی‌که قادر به استفاده از هرنوع ابزار ارتباطی کسب‌وکاری دیگر (تلفن همراه، تبلت، تلفن روی میزی، تلفن کنفرانس) متناسب با هر وضعیتی هستند. کارکنان به اطلاعات متنی مشتری و رابط ارتباطی به‌سادگی قابل استفاده زمان واقعی دسترسی دارند.
کارکنـان می‌توانند از قدرت کامل هر برنامه کاربردی کسـب‌وکاری و توانایـی برقراری ارتبـاط بومی و یکپارچه از داخل ایـن برنامه‌ها بهره برداری کنند.

2- Platform

3-Unified Communications and Collaboration UCC
4- Real- Time

شناخت چالش‌های UCC یکپارچه

در سال‌های اخیر پیشرفت شگرفی در اکو سیستم‌های ارتباطی رویداده است. نفوذ موبایل در US بیش از ۹۰٪ است و امروز موبایل رسانه مطلوب ارتباطی است. اما با کمال تعجب یک مطالعه webtorial نشان می‌دهد که ۸۵٪ کسب‌وکارها هنوز یک راهبرد سازمانی در مورد موبایل ندارند.

UCC برخی وعده‌های یکپارچه کردن ارتباطات سنتی صوتی با ارتباطات ویدیویی، پیغام‌دهی و تاحدی مرکز تماس را محقق کرده است. با این حال اکثر راه‌حل‌های موجود در بازار اساسا کارگران دانش را هدف خود قرار می‌دهند و بقیه را فراموش می‌کنند.

علیرغم پیشرفت‌های فناوری‌هایUCC، دامنه استفاده همچنان محدود و سیلویی بوده و تعداد رسانه‌های ارتباطی مانند: business phone system,business collaboration messaging system,messaging inboxes and email, business application based collaboration، در سازمان‌ها رو به رشد است. بنابراین کاربران کسب‌وکارها همچنان به ادامه مسیر، هماهنگی، همبستگی و ترجمه بین این ابزارهای مستقل می‌پردازند. این مشکلات مانع از آن می‌شود که شرکت‌ها از مزایای کامل ارتباطات یکپارچه و همکاری لازم برای رسیدن به چشم انداز ارتباطات و همکاری‌های یکپارچه (بی درز) بهره مند شوند. برخی از این چالش‌ها به شرح زیر است:

• پیام صوتی بومی، ایمیل و پیام رسانی موبایل به ندرت با زمینه کامل اتفاق می افتد

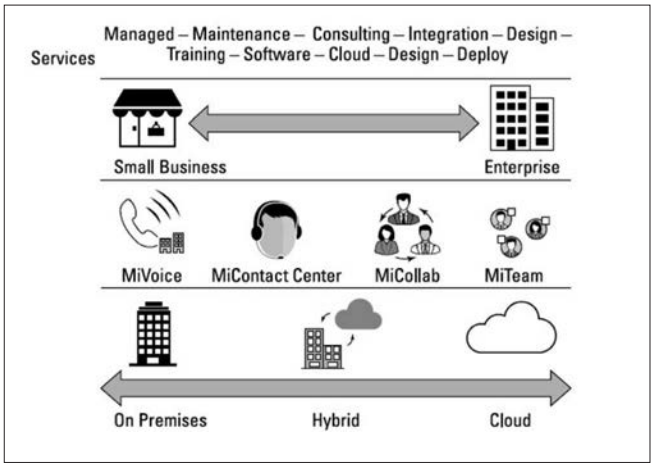
این رسانه‌های فراگیر ریشه در بازار مصرف کننده دارند. اما هم‌اکنون آن‌ها به جریان اصلی ارتباطات کسب‌وکاری مبتنی بر موبایل نیز تبدیل می‌شوند. متاسفانه در هر رخداد بدون زمینه و با قابلیت محدود برای آن زمینه که به سادگی قابل جمع آوری و در کاربردهای کسب‌وکار ذخیره شوند، ارائه می‌شوند.

• کاربردهای کسب‌وکاری و کاربردهای موبایلی کسب‌وکاری خود کانال‌های چندگانه زمینه را ایجاد می‌کنند

کاربردهای کسب‌وکاری به‌طرز چشم گیری تکامل یافته‌اند. در حالی که ارزش این کاربردها غیرقابل انکار بوده و هریک برمبنای قابلیت خود استوار است، هریک از آن‌ها به نوبه خود، حوزه دیگری از اطلاعات را برای پیمایش و مدیریت نشان می‌دهد. گاه برخی از کاربردها مولفه‌های ارتباطی در کابردهای موبایلی خود تعبیه کرده‌اند، در حالی که این گامی است در ارائه ارتباطات متنی، این پیشرفت‌ها اساسا در هربرنامه کاربردی به‌طور جداگانه، مستقل از سایر اشکال ارتباطی صورت گرفته است.

کاربردهای همکاری جریان کاری[5] تاحدی چشم انداز را ارائه می‌دهند

با هدف حل تجمع فعالیت‌های ارتباطات کسب‌وکاری، تعداد فزاینده‌ای



شکل ۵-۱: مجموعه راه‌حل‌های کامل UCC مایتل

گزینه کاربردهای همکاری جریان کاری در بازار ارائه شده است. در حالی که این کاربردها در جمع کردن ارتباطات در یک جریان کاری کانالیزه شده، موفق می‌شوند، این انباشتگی با هزینه همراه است. کاربردهای مزبور همه قابلیت‌های سایر کاربردها را تکرار نمی‌کنند و به عمد برخی قابلیت‌های نوظهور منتخب در بازار را حذف می‌کنند. کاربران این برنامه‌های کاربردی اغلب به استفاده از کاربردهای بومی خارج از کانال جریان کاری متوسل می‌شوند که موجب سردرگمی آن‌ها در انتخاب این‌که در کجا و چه کاربردی یا کانال‌هایی را برای کدام نوع ارتباطات استفاده کنند، می‌شود.

هرچه برنامه‌های کاربردی چند برابر شوند، مشکل را تقویت می‌کنند تعداد برنامه‌های کاربردی کسب‌وکاری مبتنی بر موبایل گسترش می‌یابد و تنها با افزایش ویژگی تخصصی و ماهیت کارآفرینی در نرم افزارهای کاربردی تلفن همراه به‌عنوان یک فضای ارائه دهنده خدمت، رشد آن تداوم می‌یابد. با قابلیت‌های ارتباطات زمان واقعی، بیشتر این کاربردها کارکردهای فعال شده ارتباطی را پشتیبانی می‌کنند. و درعین حال هریک، کانال ارتباطی دیگری را برای پایش و مدیریت ارائه می‌کند.

یک کارمند متوسط باید ایمیل، پیام رسان موبایلی، کانال‌های اجتماعی، CRM، کاربردهای کسب‌وکاری و نظایر آن‌ها را پایش و ردیابی کند. رشد و تکه تکه شدن کانال‌های ارتباطی کسب‌وکاری منجر به ارتباطات نادرست و غیردقیق، زمینه های کمتر متصل و سرانجام از دست دادن بهره وری کسب‌وکاری و تمرکز مشتری می‌شود.

مایتل سبد کاملی از راه‌حل‌های UCC دارد که می‌تواند در رایانش ابری، در محل یا در محیطی ترکیبی برای هر اندازه از کسب‌وکار در هر صنعت ارائه شود. شکل ۵-۱ از پژوهش ZK مجموعه قابلیت‌های خدمت و شرکای کانال برای کمک به مشتریان در هرمرحله از فرایند تحول دیجیتال را نشان می‌دهد.

5- Workstream Collaboration Application

انتشار شانزدهمین شمارهٔ مجلهٔ علوم رایانشی

شـانزدهمین شـمارهٔ مجلهٔ علوم رایانشـی، نشـریهٔ علمـی انجمن انفورماتیک ایران، در بهار ۱۳۹۹ منتشـر شد. در این شماره، ۶ مقاله به چاپ رسیده اسـت که عنوان چکیدهٔ آن‌ها برای اطلاع خوانندگان گزارش کامپیوتر در زیر آمده است:

۱-تشخیص تقلب همدست فروشنده در حین حراج با استفاده از شبیه‌سازی مبتنی بر عامل نرم‌افزاری

نویسندگان: مهران رضایی، سعید طبرسا

چکیـدهٔ مقاله: یکـی از روش‌های رایج برای خریـد و فروش کالا از طریـق حراج برخط اسـت. تعداد خریداران برخـط اینترنتی به سـرعت در حال رشد اسـت. اما مشـکل عمده‌ای که در خیلی از حراج‌های برخط مطرح می‌شـود، وجود تقلب حراج اسـت. خیلی از مشـتریان حـراج برخط، قربانـی تقلب حراج می‌شـوند، و اکثر قربانیـان تقلب حتی مدت‌هـا بعد از پایان حـراج از جریان تقلب بی‌خبر و ناآگاه می‌مانند. تقلب حراج می‌تواند به منافع فروشـنده و منافع خریدار آسـیب وارد نماید. این تحقیق بر روی تقلب حراج و روش‌های تشـخیص و جلوگیری آن تمرکز دارد. تقلب حراج انواع مختلفی داشته و تقلب خاصی که در این تحقیق مورد بررسی قرار می‌گیرد تقلب همدست فروشنده[1] نام دارد. برای تشخیص این نوع تقلب از الگوریتم نمره همدسـتی استفاده می‌شود. این الگوریتم به شـرکت‌کنندگان حراج با توجه به درجه شباهت رفتار آن‌ها نسبت به رفتارهای رایج در تقلب همدسـت فروشـنده، نمره‌ای تخصیص می‌دهد. برای این‌که شـرکت‌کننده‌ای به‌عنوان متقلب همدسـت تشـخیص داده نشـود لازم است همچون شـرکت‌کنندگان عادی رفتار کند، و در نتیجه از ارائه پیشنهادهای همدست منصرف شود. در ایـن تحقیق، عملکرد این الگوریتم با پارامترهای مختلفی مورد امتحـان قرار گرفته، و در همگی حالاتی که از پارامترهای عادی و مناسب استفاده شـده، نتایج دریافت شده حضور متقلب همدست را تشـخیص می‌دهند. از این الگوریتم می‌توانیم به‌عنوان پایه برای روش‌های تشخیص پیچیده‌تر تقلب همدست استفاده کرد.

1- Shill Bidding

۲- تشخیص موجودیت‌های اسمی بر پایه شبکه‌های عصبی با حافظه کوتاه مدّت پایدار

نویسندگان: نعیمه علی‌پور، جعفر طهمورث‌نژاد

چکیدهٔ مقاله: مسئلهٔ شناسـایی موجودیت‌های اسمی به‌عنوان یکی از شاخه‌های پردازش زبان طبیعی و زیرمجموعه‌ای از استخراج اطلاعات به‌شـمار می‌رود. هـدف اصلی در تشـخیص موجودیت‌های اسـمی، دسته‌بندی اسـامی خاص متن با برچسـب‌هایی مانند شخص، مکان و سـازمان اسـت. امروزه اکثر روش‌هایی که بـرای این منظور معرفی شـده‌اند سـعی در اسـتفاده از ویژگی‌هایی دارند کـه مختص به یک زبان خاص نیسـت. از جمله این روش‌ها می‌توان به اسـتفاده از شبکه عصبی با حافظه کوتاه مدّت پایدار اشـاره‌کرد. آموزش این شـبکه‌های عصبی به‌وسیله استخراج ویژگی‌ها از بردارهای کلمات در سطح نویسه و بردارهـای کلمات از پیش آمـوزش دیده انجام می‌گیرد. دراین مقاله مدل جدیدی برای ساخت نمایش‌های برداری کلمات پیشنهاد می‌شود که از ترکیب بردار نحوی کلمه با دو بردار کلمه قبلی به‌دسـت می‌آید. بردار نحوی کلمه شامل اطلاعات نحوی موجود در جمله مانند موقعیت کلمـه در جمله، نقـش کلمات و ارتباط نحوی آن‌ها با یکدیگر اسـت. اسـتفاده از این روش باعث توسعه سیسـتم‌هایی می‌شود که کمترین وابسـتگی را به دامنه دارند. کارایی روش پیشـنهادی بر روی مجموعه داده موجودیت‌های اسمی مورد ارزیابی قرار گرفته‌است. نتایج به‌دست آمده، نشـان‌دهنده بهبود قابل ملاحظه‌ای در مقایسه با سایر روش‌های مطرح در حوزه تشخیص موجودیت‌های اسمی می‌باشد.

۳-به‌کارگیـری پردازنـده گرافیکـی در یادگیـری ماشین: تأکید بر شبکه‌های عصبی و یادگیری عمیق

نویسندگان: فاطمه ناظمی جنابی، حمیدرضا حمیدی

چکیدهٔ مقاله: این مقاله علاوه بر مرور سـاختار پردازشـی و قابلیت‌های

پردازنده گرافیکی به تسریع‌های به‌دست آمده برای محاسبات عمومی و به‌طور خاص، شبکه‌های عصبی و یادگیری عمیق می‌پردازد. توسعه ابزارها، کتابخانه‌ها و چارچوب‌های یادگیری ماشین برای پردازنده گرافیکی همچنان نیازمند توسعه است. برای مقیاس‌پذیری روی چند پردازنده گرافیکی، موضوعاتی نظیر پشتیبانی کتابخانه‌ها و ابزارها از ارتباطات میان پردازنده‌های گرافیکی و رفع نیاز به بازنویسی کد توسط کاربر نیازمند توجه هستند. یکی از موانع محاسبات حجیم از جمله یادگیری عمیق، انرژی‌بر بودن آن‌هاست و گرایش فعلی به سمت طراحی کمک‌پردازنده‌های[2] اختصاصی است. سازندگان پردازنده‌های گرافیکی نیز با معرفی ریزمعماری وُلتا انویدیا، یک رویکرد سخت‌افزار اختصاصی در هوش مصنوعی و یادگیری ماشین در پیش گرفته‌اند. این‌گونه معماری پردازنده‌های گرافیکی (وُلتا و تورینگ) در مقایسه با سایر شتاب‌دهنده‌های سخت‌افزاری نظیر اف.پی.جی.اِی. و اِی.سیک.[3]، از حیث کارآمدی انرژی و کارایی اجرای الگوریتم‌های یادگیری عمیق قابل رقابت هستند.

۴-روش‌های شناسایی احساسات چهره، کاربردها و چالش‌ها

نویسندگان: مائدهٔ شریف‌نژاد، اسدالله شاه‌بهرامی، علیرضا آکوشیده

چکیدهٔ مقاله: در سال‌های اخیر شناسایی احساسات مختلف چهره به دلیل کاربردهای فراوان مانند تشخیص خستگی رانندگان، شناسایی وضعیت روحی بیمار، کشف دروغ و سیستم آموزش خودکار مورد توجه بسیاری در تحقیقات بینایی ماشین قرارگرفته است. به دلیل تنوع افراد و تغییرپذیری حالات چهره، شناسایی این احساسات با دقت بالا هنوز هم به‌عنوان یک مسئله چالش‌برانگیز مطرح است. در این مقاله حالات مختلف چهره مانند خشم، ترس، انزجار، شادی، غم و تعجب معرفی می‌شوند و نه پایگاه داده تصویری که در پژوهش‌های تشخیص حالات چهره مورد استفاده قرارگرفته‌اند مورد مقایسه قرار می‌گیرند. یک سیستم تشخیص حالات چهره دارای دو بخش مهم استخراج ویژگی و طبقه‌بندی حالات است. برخی از روش‌های استخراج ویژگی مانند مدل ظاهری، هیستوگرام گرادیان جهت‌دار و الگوی دودویی محلی و روش‌های طبقه‌بندی حالات چهره مانند ماشین بردار پشتیبان و شبکه عصبی پیچشی معرفی می‌شوند. مجموع مطالعات و بررسی‌ها نشان داد که روش‌های مبتنی بر شبکه عصبی پیچشی نسبت به بقیه روش‌ها دارای بالاترین دقت در تشخیص حالات چهره است. ولی تنوع داده‌های تصویر چهره از نظر سن، جنسیت، نژاد، شرایط انسداد، تغییرات روشنایی، دوری و نزدیکی و همچنین تشخیص حالات دیگر از قبیل هیجان، تأسف و خستگی از چالش‌های پیش رو است که پژوهش در این زمینه ادامه دارد.

2- Coprocessor

3- Field Programmable Gate Arrays (FPGA) & Application Specific Integrated Circuit (ASIC)

۵- ترکیب الگوریتم HITS با الگوریتم Distance Rank برای بهبود نتایج در موتورهای جستجو

نویسندگان: رعنا میلانی اباجلو، فرهاد سلیمانیان قره‌چپق

چکیدهٔ مقاله: امروزه موتورهای جستجوگر از روش‌های وب‌کاوی برای نشان دادن نتایج بهتر استفاده می‌کنند که در لیست نتایج خود پیوندهای زیادی از صفحات وب را به کاربران نمایش می‌دهند و برای بهینه و محدود کردن لیست نتایج موتورهای جستجو از الگوریتم‌های رتبه‌بندی استفاده می‌شود. در این مقاله یک روش جدید که ترکیبی از الگوریتم HITS با الگوریتم Distance Rank است برای بهبود نتایج در موتورهای جستجو ارائه‌شده است که در روش پیشنهادی از فرایند اصلی الگوریتم Distance Rank برای بهبود الگوریتم HITS استفاده شده است. مشکل اصلی الگوریتم HITS این است که رتبه‌بندی صفحات وب براساس میزان ارتباط آن‌ها با پرس وجوی کاربر است. اما در الگوریتم Distance از فاصله لگاریتمی میان صفحات به منظور رتبه‌بندی استفاده می‌شود. ارزیابی روش پیشنهادی بر روی سه مجموعه داده شامل گراف استاندارد، گراف تصادفی، گراف دانشگاه آزاد اسلامی واحد ارومیه انجام گرفته که نتایج نشان می‌دهد که روش پیشنهادی در مقایسه با الگوریتم‌های دیگر عملکرد بهتری دارد و توانسته است رتبه‌بندی متفاوت و بهتری نسبت الگوریتم پایه HITS و سایر الگوریتم‌های رتبه‌بندی مانند Distance Rank و PR و WPR داشته باشد. همچنین الگوریتم‌های پیشنهادی برمبنای معیارهای AP، P@n و NDC مورد ارزیابی قرار گرفت که نتایج نشان می‌دهد که روش پیشنهادی به ترتیب مقدار ۱ و ۱ و ۸/۱ را به دست آورده است.

۶- تنظیم قوت ته‌نقش در ته‌نقش‌گذاری وفقی تصاویر دیجیتال با استفاده از اتوماتای یادگیر سلولی

نویسندگان: سعید ابراهیم‌زاده، علی‌محمد لطیف، زینب مهرنهاد

چکیدهٔ مقاله: سامانه‌های ته‌نقش‌گذاری[4] تصویر در هر کاربرد به ویژگی‌های خاصی نیاز دارند. از مهم‌ترین ویژگی‌های مشترک این سامانه‌ها شفافیت و مقاومت است. شفافیت و مقاومت به ضریبی به نام قوت ته‌نقش[5] وابسته است. در اثر افزایش قوت ته‌نقش مقاومت افزایش و شفافیت کاهش می‌یابد و لذا داشتن دو ویژگی مقاومت و شفافیت به‌طور هم‌زمان امکان‌پذیر نیست و باید با انتخاب قوت ته‌نقش مناسب، مصالحه‌ای بین این دو ویژگی برقرار کرد. در این مقاله با استفاده از اتوماتای سلّولی یادگیر، الگوریتمی ارائه شده است که تابع برازندگی پیشنهادی را افزایش داده و قوت ته‌نقش مناسب را جست‌وجو می‌کند. نتایج آزمایش‌ها نشان می‌دهد که الگوریتم پیشنهادی جواب‌های مناسبی را در مقایسه با روش ژنتیک تولید می‌کند.

4- watermarking

5- watermark

مروری بر استاندارد بین‌المللی ایزو ۲۷۷۹۹: انفورماتیک سلامت

مدیریت امنیت اطلاعات در حوزهٔ سلامت با استفاده از ایزو ۲۷۰۰۲

فاطمه قربانی

دانشجوی کارشناسی ارشد مهندسی فناوری اطلاعات گرایش معماری سازمانی، آزمایشگاه معماری سازمانی، دانشگاه صنعتی شیراز

پست الکترونیکی: f.ghorbani88@gmail.com

سیدرئوف خیامی

هیئت علمی دانشکده مهندسی کامپیوتر و فناوری اطلاعات، آزمایشگاه معماری سازمانی، دانشگاه صنعتی شیراز

پست الکترونیکی: khayami@sutech.ac.ir

چکیده

در حالی که محافظت و امنیت اطلاعات شخصی برای تمام افراد، شرکت‌ها، موسسات و دولت‌ها مسئله مهمی محسوب می‌شود، در بخش سلامت به علت ویژگی‌های منحصربه فرد این حوزه این اهمیت دوچندان شده و الزامات خاصی وجود دارد که برای تضمین محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات پزشکی شخصی باید محقق شوند. استاندارد ایزو ۲۷۷۹۹ اولین بار در سال ۲۰۰۸ و برای مدیریت امنیت اطلاعات در حوزهٔ بهداشت و درمان منتشر شد. آخرین نسخه این استاندارد در سال ۲۰۱۶ و برای هم راستایی با انتشار استانداردهای ایزو۲۰۱۳:۲۷۰۰۱ و ۲۰۱۳:۲۷۰۰۲ منتشر گردید.

این استاندارد برای استفاده از استانداردهای امنیت اطلاعات سازمانی و شیوه‌های مدیریت امنیت اطلاعات، از جمله انتخاب، پیاده‌سازی و مدیریت کنترل‌ها در محیط‌های بهداشتی-درمانی دستورالعمل‌هایی ارائه می‌دهد. این استاندارد با تعریف این دستورالعمل‌ها درواقع از تفسیر و اجرای ایزو ۲۷۰۰۲ پشتیبانی می‌کند و یک همراه برای این استاندارد بین‌المللی محسوب می‌شود. با اجرای ایزو ۲۷۷۹۹ سازمان‌های حوزهٔ بهداشت و درمان و سایر متولیان اطلاعات سلامت می‌توانند به حداقل سطح امنیتی که مناسب شرایط سازمان بوده و حافظ محرمانگی، یکپارچه‌سازی و دسترسی‌پذیری اطلاعات پزشکی شخصی است دست یابند.

مقدمه

بهداشت و درمان یک سازمان وابسته به دانش و اطلاعات است و ارائه‌دهندگان خدمات بهداشتی-درمانی برای کسب، مدیریت، تحلیل و انتشار اطلاعات بهداشتی-درمانی وابستگی روزافزون به فناوری اطلاعات (IT) دارند. راه‌حل‌های IT به‌عنوان ابزار بهبود تصمیم‌گیری و ترویج تبادل اطلاعات به‌کار گرفته می‌شوند تا اثربخشی موسسات بهداشتی-درمانی را ارتقا داده و اطلاعات بیماران را به‌صورت الکترونیکی جمع‌آوری نمایند. اطلاعاتی که در ارتباط با سلامت

بیمار جمع‌آوری می‌شود، اطلاعات پزشکی شخصی نامیده می‌شود. اطلاعات پزشکی شخصی شامل اطلاعات سلامت فرد، ناتوانی‌ها، وضعیت استفاده از خدمات درمانی و سایر اطلاعات شخصی مرتبط می‌باشد.

با وجود این که امنیت اطلاعات شخصی و محافظت از آن‌ها برای تمام افراد، شرکت‌ها، موسسات و حاکمیت‌ها حائز اهمیت است، اما در بخش سلامت نیازمندی‌هایی وجود دارد که برآورده نمودن آن‌ها برای تضمین محرمانگی، یکپارچگی، حسابرسی و دسترسی‌پذیری اطلاعات پزشکی شخصی ضروری است. از نظر بسیاری از صاحب نظران، این نوع اطلاعات جزء محرمانه‌ترین انواع اطلاعات شخصی هستند. در صورت نیاز به حفظ حریم خصوصی بیماران تحت مراقبت حفظ این محرمانگی ضروری است. برای تضمین ایمنی بیمار باید یکپارچگی اطلاعات پزشکی حفظ شود و مولفه مهم این محافظت، تضمین قابلیت حسابرسی روی کل چرخه اطلاعات است. دسترسی‌پذیری اطلاعات پزشکی نیز برای تحویل موثر مراقبت بهداشتی حیاتی است. سیستم‌های انفورماتیک سلامت برای این که در مواجهه با بلایای طبیعی، نقص سیستم و حملات انکار سرویس عملیاتی باقی بمانند باید درخواست‌های منحصر به فردی را برآورده نمایند. بنابراین حفظ محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات پزشکی به خبرگی در بخش بهداشت و درمان نیاز دارد. تمام سازمان‌های حوزهٔ بهداشت و درمان، صرف نظر از اندازه، مکان و مدل تحویل سرویس، باید برای محافظت از اطلاعات پزشکی که در اختیار دارند کنترل‌های سخت‌گیرانه‌ای داشته باشند. بنابراین سازمان‌های بهداشتی-درمانی در انتخاب و اجرای چنین کنترل‌هایی به دستورالعمل‌های واضح، مختصر و خاص حوزه بهداشت و درمان نیاز دارند.

استاندارد بین‌المللی ایزو ۲۷۷۹۹ برای سازمان‌های حوزه بهداشت و درمان و سایر متولیان اطلاعات پزشکی شخصی و در خصوص بهترین روش محافظت از محرمانگی، یکپارچگی و دسترسی‌پذیری این اطلاعات دستورالعمل‌هایی ارائه می‌دهد. این استاندارد اساسا مبتنی بر دستورالعمل کلی است که در استاندارد ایزو ۲۷۰۰۲ ارائه می‌شود و درواقع با تمرکز روی الزامات امنیتی حوزهٔ سلامت و محیط‌های اجرایی منحصر به فرد آن این استاندارد را توسعه داده است. این استاندارد برای طیف وسیعی از سازمان‌های بهداشتی-درمانی، صرف نظر از اندازه، مکان و مدل‌های تحویل سرویس در این سازمان‌ها، قابل اجراست. با افزایش تبادل الکترونیکی اطلاعات پزشکی شخصی میان متخصصین حوزهٔ سلامت (مثل استفاده از سرویس‌های بی‌سیم و اینترنت)، اتخاذ یک مرجع مشترک برای مدیریت امنیت اطلاعات در بخش بهداشت و درمان یک مزیت بدیهی محسوب می‌شود.

در ادامه این نوشتار در بخش اول معرفی مختصری از سازمان بین‌المللی استانداردسازی، موسوم به ایزو، ارائه می‌شود. سپس در بخش دوم به معرفی استاندارد ایزو ۲۷۷۹۹، ارتباط آن با سایر استانداردها، اهداف، موضوعات تحت پوشش، مخاطبین و مزایا آن پرداخته می‌شود. در بخش سوم نحوه استفاده از این استاندارد بیان می‌شود. در بخش چهارم مروری مختصر بر ساختار این استاندارد ارائه می‌شود.

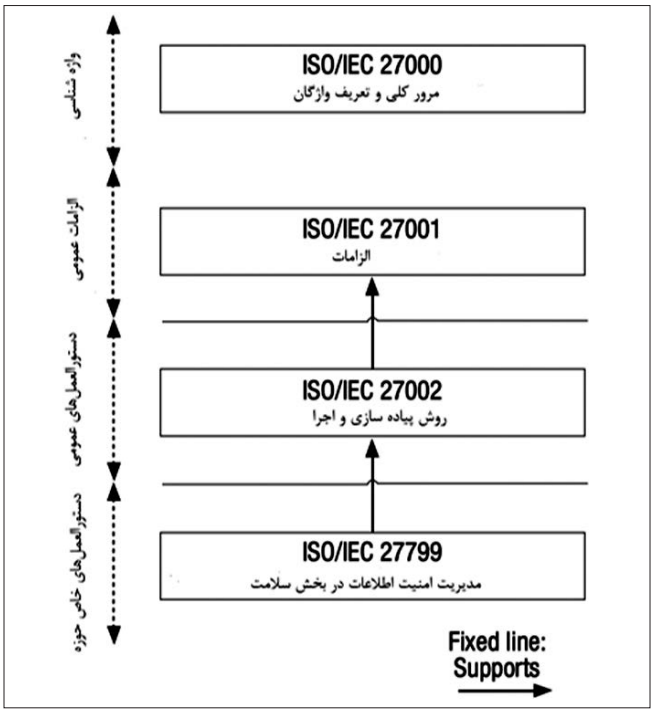
۱- معرفی ایزو

سازمان بین‌المللی استانداردسازی (The International Organization for Standardization) که معمولاً به نام ایزو (ISO) شناخته می‌شود، مؤسسه بین‌المللی تعیین استاندارد است که از نمایندگان موسسات ملی استانداردسازی تشکیل شده است. این سازمان غیردولتی در سطح وسیعی به وضع استانداردهای کلی و جزئی می پردازد و هدف آن هماهنگ‌کردن استانداردهای متفاوت جهانی است. در عمل ایزو به‌صورت کنسرسیومی که دارای ارتباطات قوی با دولت‌ها است، فعالیت می‌کند. این مؤسسه انواع استانداردهای تجاری و صنعتی جهانی را تعیین می‌نماید. مرکز ایزو در ژنو سویس قرار دارد.

سازمان بین‌المللی استانداردسازی، با آن‌که یک سازمان غیردولتی است اما از بیشتر سازمان‌های غیردولتی قدرتمندتر است. این قدرت از پذیرش جهانی و حمایت کشورهای عضو آن به دست آمده است تا آن جا که استانداردهای این مؤسسه در کشورهای عضو به قانون تبدیل می‌شود. امروزه نزدیک به ۱۶۴ کشور در این سازمان به عضویت درآمده‌اند که ایران نیز یکی از آن‌هاست.

۲- معرفی استاندارد بین‌المللی ایزو ۲۷۷۹۹

استاندارد بین‌المللی ایزو ۲۷۷۹۹ که تحت عنوان انفورماتیک سلامت- مدیریت امنیت اطلاعات پزشکی با استفاده از ایزو ۲۷۰۰۲ تعریف شده است، یکی از استانداردهای خانواده ایزو ۲۷۰۰۰ (که تحت عنوان «استانداردهای خانواده ISMS» یا به‌طور خلاصه «ISO27k» نیز شناخته می‌شوند) می‌باشد. استانداردهای خانواده ایزو ۲۷۰۰۰ از استانداردهای امنیت اطلاعاتی تشکیل شده‌اند که مشترکا توسط سازمان بین‌المللی استانداردسازی (ISO) و کمیته بین‌المللی الکترونیک (IEC) منتشر شده‌اند. مشابه با طراحی سیستم‌های مدیریت برای تضمین کیفیت (مجموعه ISO9000)، محافظت محیطی ISO 14000)) و سایر سیستم‌های مدیریتی، مجموعه استانداردهای ایزو ۲۷k در چارچوب یک سیستم کلی مدیریت امنیت اطلاعات (ISMS) به ارائهٔ توصیه‌های مبتنی بر بهروش در حوزهٔ مدیریت امنیت اطلاعات - مدیریت ریسک‌های اطلاعات از طریق کنترل‌های امنیت اطلاعات- می پردازد. از تمام سازمان‌ها خواسته می‌شود که ریسک‌های اطلاعاتی خود را ارزیابی کنند، سپس براساس نیازهایشان و با استفاده از دستورالعمل‌ها و پیشنهادها مرتبط با آن‌ها برخورد کنند (عموما از طریق کنترل‌های امنیت اطلاعات). با توجه به ماهیت پویا امنیت و ریسک اطلاعات،



شکل ۱: ارتباط ایزو ۲۷۷۹۹ با سایر استانداردهای خانواده ایزو ۲۷k

مفهوم ISMS در پاسخ به تغییرات در تهدیدات، آسیب‌پذیری‌ها و تاثیرات وقایع، اقدام به ادغام بازخورد مستمر و فعالیت‌های بهبود می‌کند. این مجموعه تعمدا دامنه گسترده‌ای دارد تا بیش از فقط حریم خصوصی، محرمانگی و موضوعات مرتبط با فناوری اطلاعات و امنیت سایبری را تحت پوشش قرار دهند. استانداردهای این مجموعه فارغ از اندازه و شکل سازمان قابل اجرا هستند.

۲-۱- ارتباط استاندارد ایزو ۲۷۷۹۹ با سایر استانداردها

برای درک ایزو ۲۷۷۹۹ آشنایی با ایزو ۲۷۰۰۲ ضروری است. در حال حاضر ایزو ۲۷۰۰۲ به‌طور گسترده ای برای مدیریت امنیت فناوری اطلاعات در انفورماتیک سلامت و از طریق آژانس ملی یا دستورالعمل‌های منطقه‌ای در استرالیا، کانادا، فرانسه، هلند، نیوزلند، آفریقای جنوبی، انگلیس و غیره مورد استفاده قرار می‌گیرد. ایزو ۲۷۷۹۹ بر پایه تجربیات به دست آمده از این تلاش‌های ملی در حوزه امنیت اطلاعات پزشکی شخصی طراحی شده است و به‌عنوان یک سند همراه برای ایزو ۲۷۰۰۲ در نظر گرفته می‌شود. هدف این استاندارد تغییر مجموعه استانداردهای ایزو ۲۷۰۰۰ نیست و در عوض یک مکمل برای این استانداردهای عام محسوب می‌شود. ایزو ۲۷۷۹۹ ایزو ۲۷۰۰۲ را در حوزه بهداشت و درمان اجرا می‌کند، به این معنا که کاربرد مناسب کنترل‌های امنیتی در محافظت از اطلاعات پزشکی شخصی را به دقت مورد توجه قرار می‌دهد. در برخی از موارد، این ملاحظات مولفین استاندارد ایزو ۲۷۷۹۹ را به این نتیجه می‌رساند که برای محافظت کافی از اطلاعات پزشکی شخصی استفاده از برخی اهداف کنترلی ایزو ۲۷۰۰۲ ضروری است. بنابراین ایزو ۲۷۷۹۹ براساس به‌کارگیری برخی از کنترل‌های امنیتی که در ایزو ۲۷۰۰۲ مشخص شده‌اند قیود را تعریف می‌کند.

تمام کنترل‌های امنیتی که در ایزو ۲۷۰۰۲ شرح داده شده‌اند با انفورماتیک سلامت مرتبط هستند اما نحوه به‌کارگیری برخی از کنترل‌ها در راستای محافظت از محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات پزشکی نیازمند توضیح بیشتری است. همچنین نیازمندی‌های دیگری وجود دارند که خاص بخش سلامت هستند. از این رو استاندارد ۲۷۷۹۹ دستورالعمل دیگری ارائه می‌دهد، به شکلی که افراد مسئول امنیت اطلاعات پزشکی بتوانند آن‌ها را به راحتی درک نموده و اتخاذ نمایند.

سازمان‌های بهداشتی-درمانی (مثلا یک بیمارستان) می‌توانند با استفاده از ایزو ۲۷۰۰۱ و بدون نیاز به گواهی‌نامه یا حتی تایید ایزو ۲۷۷۹۹ گواهی بگیرند. با این حال سازمان ایزو امیدوار است که موازی با تلاش سازمان‌های بهداشتی-درمانی برای ارتقاء امنیت اطلاعات پزشکی شخصی، مطابقت با ایزو ۲۷۷۹۹ نیز به‌عنوان یک استاندارد دقیق‌تر در حوزهٔ بهداشت و درمان فراگیرتر شود. شکل ۱ نحوهٔ ارتباط این استاندارد با سایر استانداردهای مجموعه ایزو ۲۷k را نشان می‌دهد.

۲-۲- دامنهٔ پوشش دهی

ایزو ۲۷۷۹۹ و ایزو ۲۷۰۰۲ در کنار هم تمام نیازمندی‌های مرتبط با امنیت اطلاعات در حوزهٔ بهداشت و درمان را تعریف می‌کنند. این استانداردها روی نحوهٔ برآورده شدن این نیازمندی‌ها تعریفی ندارند، به‌عبارت دیگر از نظر فناوری بی‌طرف هستند. بی‌طرفی نسبت به پیاده‌سازی فناوری‌ها یک ویژگی مهم این استانداردهاست. فناوری امنیت همچنان تحت توسعه سریع قرار دارد و سرعت این تغییر در حال حاضر به جای سالیانه، ماهانه اندازه‌گیری می‌شود. در مقابل، با وجود بازبینی‌های دوره‌ای استانداردهای بین‌المللی، در حالت کلی انتظار می‌رود که یک استاندارد برای سال‌ها معتبر باشد. از سوی دیگر، بی‌طرفی فنی باعث می‌شود فروشندگان و ارائه‌دهندگان سرویس در پیشنهاد فناوری‌های جدید یا در حال توسعه برای برآورده ساختن الزامات ایزو ۲۷۷۹۹ آزاد باشند.

حوزه‌های زیر گرچه در محدودهٔ امنیت اطلاعات می‌گنجند اما خارج از محدوده ایزو ۲۷۷۹۹ هستند:

۱- متدولوژی‌ها و آزمایش‌های آماری برای ناشناس ماندن اطلاعات پزشکی شخصی

۲- متدولوژی‌هایی برای نام مستعار اطلاعات پزشکی شخصی

۳- کیفیت شبکه سرویس و شیوه‌های اندازه‌گیری دسترسی‌پذیری شبکه‌های مورداستفاده برای انفورماتیک سلامت

۲-۳- اهداف

حفظ محرمانگی، دسترسی‌پذیری و یکپارچگی (شامل معتبر بودن، پاسخگویی، حسابرسی) اهداف فراگیر امنیت اطلاعات هستند.

در حـوزه بهداشـت و درمان، حفظ حریم شـخصی بیماران به حفظ محرمانگی اطلاعات پزشـکی شخصی بسـتگی دارد. یکی از اقداماتی کـه انجام آن برای حفظ محرمانگی ضروری اسـت، حفظ یکپارچگی داده‌هاسـت، زیرا از بین رفتن یکپارچگی داده‌های کنترل دسترسی، مسـیرهای حسابرسی و سـایر داده‌های سیسـتم امکان وقوع نقض محرمانگی را فراهم نموده و یا باعث می‌شـود نقض محرمانگی دور از نظر قـرار بگیرد. علاوه بر این، ایمنی بیماران نیز به حفظ یکپارچگی اطلاعات پزشکی شخصی بسـتگی دارد و شکست در این یکپارچگی می‌تواند منجر به بیماری، آسیب و یا حتی مرگ شود.

یکـی دیگـر از ویژگی‌هـای بسـیار مهم در سیسـتم‌های سـلامت دسترسـی‌پذیری سـطح بالا است. در این سیسـتم‌ها معمولا درمان فرآیندی اسـت که زمان نقش حیاتی در آن دارد. در واقع بلایایی که می‌توانند منجر به قطع سیسـتم‌های فنـاوری اطلاعات غیرمرتبط با سلامت شوند در بسیاری از مواقع زمان‌هایی رخ می‌دهند که اطلاعات موجود در سیسـتم‌های سلامت به شـدت موردنیاز هستند. از سوی دیگر، حملات انکار سرویس روی سیستم‌های تحت شبکه بسیار رایج هستند.

کنترل‌هایی که در این استاندارد موردبحث قرار می‌گیرند کنترل‌هایی هستند که برای حفاظت از محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات پزشـکی شـخصی و اطمینـان از این که دسترسـی به این اطلاعات قابل پیگیری و پاسـخگویی اسـت مناسـب تشخیص داده شده‌اند.

ایـن کنترل‌هـا به اجتناب از وقـوع خطا در اقدامات پزشـکی کمک می‌کنند، خطاهایی که ممکن اسـت ناشـی از عدم حفظ یکپارچگی اطلاعات پزشکی باشند. علاوه بر این، استمرار سرویس‌های پزشکی با کمک این کنترل‌ها تضمین می‌شوند.

از دیگـر اهداف امنیت اطلاعات در حوزهٔ بهداشـت و درمان می توان به موارد زیر اشاره نمود:

۱- احتـرام به تعهدات قانون‌گـذار، آن چنان که در قوانین و مقررات مربـوط به محافظت از داده‌ها بیان شـده‌اند و از حق حریم خصوصی بیمار محافظت می‌کنند.

۲- حفـظ بهروش‌هایی که در ارتباط بـا امنیت و حریم خصوصی در انفورماتیک سلامت به تثبیت رسیده‌اند.

۳- حفظ پاسخگویی فردی و سازمانی در میان سازمان‌های بهداشتی-درمانی و متخصصین سلامت

۴- پشـتیبانی از اجرای مدیریت سامانمند ریسک درون سازمان‌های بهداشتی-درمانی

۵- برآورده نمودن نیازهای امنیتی که در موقعیت‌های رایج بهداشت ودرمان شناسایی شده‌اند

۶- کاهش هزینه‌های عملیاتی با تسـهیل به‌کارگیری بیشتر فناوری به شـیوه‌ای امن، ایمن و خوب مدیریت شده که در عین پشتیبانی از فعالیت‌های بهداشتی- درمانی آن‌ها را محدود ننماید.

۷- حفـظ اعتمـاد عمومـی بـه سـازمان‌های بهداشـتی-درمانی و سیستم‌های اطلاعاتی که این سازمان‌ها به آن‌ها متکی هستند.

۸- حفظ معیارها و اصول اخلاقی حرفه‌ای مطابق با آن چه که توسط سـازمان‌های حرفه‌ای مرتبط با سلامت ایجاد شـده‌اند (تا آن جا که امنیـت اطلاعات حافـظ محرمانگی و یکپارچگی اطلاعات پزشـکی باشد).

۹- اداره کردن سیستم‌های اطلاعات سلامت الکترونیکی در محیطی که به خوبی در برابر تهدیدات ایمن شده باشد.

۱۰- تشـخیص قابلیت همکاری میان سیستم‌های سلامت، به‌طوری که اطلاعات پزشکی به‌طور فزاینده‌ای در میان سازمان‌ها و در سراسر مرزهـای قضایـی جریان یابد (مخصوصـا آن چنان کـه این قابلیت همکاری مدیریت مناسب اطلاعات پزشکی را ارتقا دهد تا محرمانگی، یکپارچگی و دسترسی‌پذیری مستمر به آن‌ها تضمین شود).

۲-۴- ارتباط ایزو ۲۷۷۹۹ با حاکمیت اطلاعات، حاکمیت شرکتی و حاکمیت بالینی

با وجود این که ممکن اسـت سـازمان‌های بهداشتی -درمانی نسبت به جایگاهشـان در حاکمیت بالینی و حاکمیت شرکتی با هم تفاوت داشـته باشـند، اما بایـد اهمیـت یکپارچگی و حضـور در حاکمیت اطلاعـات، به‌عنوان یک پشـتیبان حیاتی برای هـر دو گروه، فراتر از بحث و گفتگو باشـد. از آن جایی که سـازمان‌های بهداشتی-درمانی برای پشتیبانی از تحویل مراقبت روز به روز به سیستم‌های اطلاعاتی وابسته‌تر می‌شوند (مثلا با به‌کارگیری فناوری‌های پشتیبانی از تصمیم و گرایش به سـمت بهداشـت و درمان «مبتنی بر شـواهد» به جای بهداشت و درمان «مبتنی بر تجربه»)، ثابت شده است که رویدادهایی که به موجب آن‌ها یکپارچگی، دسترسـی‌پذیری و محرمانگی از بین می‌رود می‌توانند تاثیر بالینی قابل توجهی داشـته و مشکلات برآمده از ایـن تاثیرات، نقض در تعهدات اخلاقی و قانونی ذاتی یک «وظیفه مراقبتی» را به دنبال خواهند داشت.

تمام کشـورها و حوزه‌هـای قضایی دارای مطالعات موردی هسـتند که در آن‌ها چنین شـکاف‌هایی منجر به تشـخیص نادرسـت، مرگ یا بهبودهای طولانی مدت شـده‌اند. بنابراین چارچوب‌های حاکمیت بالینـی باید با درجـه اهمیتی برابر بـا اهمیت برنامه‌هـای درمانی، راهبردهای مدیریت عفونت و سـایر موضوعـات مهم مدیریت بالینی با مسـئلهٔ مدیریت موثر ریسک امنیت اطلاعات رفتار کند. استاندارد ایزو ۲۷۷۹۹ به مسـئولین حاکمیت بالینـی کمک می‌کند که درک مناسبی از سهم کاربردی راهبردهای موثر امنیت اطلاعات در سازمان داشته باشند.

۲-۵- مخاطبان

این اسـتاندارد برای مسـئولین نظارت بر امنیت اطلاعات پزشـکی، مسـئولین سـازمان‌های بهداشتی-درمانی و سـایر متولیان اطلاعات پزشـکی که دسـتورالعمل‌های این حـوزه را دنبـال می‌کنند و نیز

مشاورین امنیتی آن‌ها، ممیزها، فروشندگان و ارائه‌دهندگان سرویس تدوین شده است.
مولفین این استاندارد نه قصد دارند مبانی اولیه امنیت کامپیوتر را تشریح کنند و نه می‌خواهند آنچه در ایزو ۲۷۰۰۲ نوشته شده است را مجددا بیان کنند. تعداد زیادی نیازمندی امنیتی وجود دارد که برای تمام سیستم‌های کامپیوتری مشترک هستند، چه آن‌هایی که در سیستم‌های مالی استفاده می‌شوند، چه در تولید، کنترل صنعتی یا در واقع در هر تلاش سازمان یافته دیگری. در ایزو ۲۷۷۹۹ در واقع یک تلاش منسجم برای تمرکز روی نیازمندی‌های امنیتی مرتبط با چالش‌های منحصربه فرد تحویل الکترونیکی اطلاعات پزشکی است.

۲-۶- مزایا

استاندارد ۲۷۰۰۲ یک استاندارد بین‌المللی گسترده و پیچیده است و توصیه‌هایی که در آن آمده مخصوص حوزهٔ بهداشت و درمان نیست. ایزو ۲۷۷۹۹ امکان اجرای پایدار ایزو ۲۷۰۰۲ در محیط‌های بهداشتی-درمانی را فراهم می‌کند و در این اجرا چالش‌های منحصر به فرد بخش سلامت را موردتوجه قرار می‌دهد. با دنبال کردن این استاندارد سازمان‌های بهداشتی-درمانی می‌توانند از حفظ محرمانگی و یکپارچگی داده‌ها، دردسترس باقی ماندن سیستم‌های اطلاعات پزشکی و تقویت پاسخگویی اطمینان حاصل کنند.
اتخاذ این استاندارد بین‌المللی از سوی سازمان‌های بهداشتی-درمانی، هم در داخل سازمان و هم در میان سازمان‌ها، به افزایش قابلیت همکاری کمک کرده و استفاده ایمن از فناوری‌های جدید در تحویل مراقبت بهداشتی را امکان‌پذیر می‌کند. به اشتراک‌گذاری این اطلاعات و در عین حال حفظ حریم خصوصی می‌تواند خروجی‌های بهداشت و درمان را به‌طور چشم‌گیری بهبود دهد.
در نتیجهٔ اجرای این استاندارد، سازمان‌های بهداشتی-درمانی می‌توانند انتظار کاهش تعداد وقایع امنیتی و شدت آن‌ها را داشته باشند و این اجازه می‌دهد از منابع سازمان برای فعالیت‌های مولد استفاده شود. به این ترتیب امنیت فناوری اطلاعات امکان استقرار مقرون به صرفه و مولد منابع بهداشت و درمان را فراهم خواهد کرد. در واقع، پژوهش انجام شده توسط انجمن امنیت اطلاعات و تحلیل‌گران بازار نشان داده است که یک امنیت خوب و همه جانبه می‌تواند تاثیر مثبت بیش از ۲ درصدی روی نتایج سازمان‌ها داشته باشد.
در نهایت، یک رویکرد ثابت برای امنیت اطلاعات، که برای تمام گروه‌های درگیر در بهداشت و درمان قابل درک باشد، موجب ارتقاء روحیه کارکنان و افزایش اعتماد عموم مردم به سیستم‌های اطلاعات پزشکی شخصی می‌شود.

۲-۷- ساختار ایزو ۲۷۷۹۹

استاندارد ایزو ۲۷۷۹۹ در انتشار اولیه دارای ۷ بند، ۳ پیوست و یک کتابشناسی بود (به جز پیشگفتار و مقدمه)، اما در نسخه دوم که سال ۲۰۱۳ منتشر شد جهت حفظ هم راستایی با استاندارد ایزو۲۷۰۰۲، این تعداد به ۱۸ بند افزایش یافتند (بدون در نظر گرفتن پیشگفتار و مقدمه). شماره و عنوان هر بند کاملا مانند ساختار ایزو ۲۷۰۰۲ قرار داده شده است. بعد از معرفی کوتاه سازمان بین‌المللی استانداردسازی (ایزو) در بخش پیشگفتار و معرفی ایزو ۲۷۷۹۹ و تبیین موضوعاتی چون رویکرد کلی استاندارد، اهداف، مزایا، گروه مخاطبین، دامنه هدف و غیره در بخش مقدمه، سند استاندارد به شکلی که در جدول ۱ نشان داده شده است سازماندهی شده است.

۲-۸- نحوه استفاده از ایزو ۲۷۷۹۹

قبل از مطالعهٔ این استاندارد لازم است که آشنایی مناسبی با بندهای مقدماتی ایزو ۲۷۰۰۲ وجود داشته باشد و مجریان استاندارد نیز باید ایزو ۲۷۰۰۲ را به‌طور کامل مطالعه نمایند چرا که در متن ایزو ۲۷۷۹۹ مکررا به بندهای مرتبط در ایزو ۲۷۰۰۲ ارجاع داده شده و از این رو بدون دسترسی به متن کامل ایزو ۲۷۰۰۲ درک استاندارد موردبحث امکان پذیر نخواهد بود.
طبقه‌بندی کنترل‌های امنیتی در ایزو ۲۷۷۹۹ همانند ایزو ۲۷۰۰۲ است و با همان شماره و عنوان فصل که در ایزو ۲۷۰۰۲ سازماندهی شده‌اند در ایزو ۲۷۷۹۹ نیز مشاهده می‌شوند. بنابراین ایزو ۲۷۷۹۹ نیز همانند ایزو ۲۷۰۰۲ دارای ۱۸ فصل است. در نهایت این استاندارد بین‌المللی با ۳ پیوست و یک کتابشناسی به پایان می‌رسد.
پیوست A تهدیدات عمومی اطلاعات پزشکی را تشریح می‌کند.
افرادی که به دنبال دستورالعمل پیاده‌سازی ۲۷۰۰۲ در یک محیط بهداشتی-درمانی هستند با مراجعه به پیوست B یک طرح اقدام عملی خواهند یافت. در این پیوست هیچ نیازمندی اجباری قرار داده نشده است و تنها یک دستورالعمل کلی درخصوص بهترین شیوهٔ پیاده‌سازی ایزو ۲۷۰۰۲ در بخش سلامت ارائه شده است. این بخش از استاندارد ایزو ۲۷۷۹۹ حول چرخه‌ای از فعالیت‌ها (برنامه‌ریزی/انجام/بررسی/اقدام) که در ایزو ۲۷۰۰۱ شرح داده شده‌اند حرکت می‌کند و دنبال کردن آن پیاده‌سازی قدرتمند یک سیستم مدیریت امنیت اطلاعات را نتیجه می‌دهد.
پیوست C حاوی یک ماتریس خودارزیاب در راستای انطباق است.
بخش کتابشناسی سایر استانداردهای مرتبط با امنیت اطلاعات پزشکی را لیست می‌کند.

۳- مفاهیم مرتبط با امنیت اطلاعات

۳-۱- امنیت اطلاعات

اطلاعات یک دارایی است که همانند سایر دارایی‌های تجاری مهم برای کسب‌وکار سازمان ضروری بوده و در نتیجه نیازمند محافظت مناسب است. در محیط‌های تجاری که به هم پیوستگی فزاینده‌ای دارند این اهمیت دوچندان می‌شود. این به هم پیوستگی فزاینده باعث شده است که اطلاعات در معرض تعداد روزافزون و انواع گسترده ای از تهدیدات و آسیب‌پذیری‌ها قرار بگیرند.

جدول ۱-:ساختار ایزو ۲۷۷۹۹

شماره بند	عنوان	توضیح
۱	دامنه	توضیح بخش‌هایی از امنیت اطلاعات که در این استاندارد پوشش داده می‌شوند و فهرست بخش‌هایی که خارج از محدودهٔ تعریف شده برای این استاندارد هستند
۲	منابع هنجاری	معرفی اسنادی که در اجرای این سند نقش کلیدی دارند
۳	اصطلاحات و تعاریف	تعریف واژگان و اصطلاحاتی که در تالیف این استاندارد مورد استفاده قرار گرفته‌اند. بخشی از این تعاریف و اصطلاحات مربوط به دامنهٔ تحت پوشش استاندارد (بخش بهداشت و درمان) می‌گردد و بخشی دیگر واژگان مرتبط با امنیت اطلاعات هستند.
۴	ساختار استاندارد	
۵	سیاست‌های امنیت اطلاعات	شامل مباحثی پیرامون جهت‌گیری مدیریت برای امنیت اطلاعات و بازبینی سیاست‌های امنیت اطلاعات
۶	سازمان امنیت اطلاعات	پرداختن به نقش‌ها و مسئولیت‌های مرتبط با امنیت اطلاعات، تفکیک وظایف و امنیت اطلاعات در مدیریت پروژه برای سازمان داخلی و سیاست استفاده از دستگاه‌های موبایل و دورکاری به‌عنوان بخش خارجی سازمان
۷	امنیت منابع انسانی	ایزو ۲۷۷۹۹ امنیت در این حوزه را به سه بخش تقسیم می‌کند: پیش از استخدام، در حین استخدام، قطع و یا تغییر همکاری. در بخش اول غربالگری و شرایط استخدام مطرح می‌شود. در بخش دوم به مسئولیت‌های مدیریت و آموزش امنیت اطلاعات پرداخته می‌شود. در بخش سوم نیز مسئولیت‌های امنیتی مربوط به قطع یا تغییر همکاری عنوان می‌گردد
۸	مدیریت دارایی	تهیه فهرستی از دارایی‌های موجود، تعیین مالکیت دارایی‌ها، تعریف استفاده قابل قبول از دارایی‌ها، طبقه‌بندی اطلاعات، برچسب دهی به اطلاعات، مدیریت رسانه‌های قابل جابه‌جایی حذف و انتقال فیزیکی رسانه از جمله مباحث مطرح شده در این فصل از استاندارد ۲۷۷۹۹ می‌باشند
۹	کنترل دسترسی	الزامات کسب‌وکار برای کنترل دسترسی، سیاست کنترل دسترسی، دسترسی به شبکه‌ها و سرویس‌های شبکه، مدیریت دسترسی کاربر، مدیریت مجوزهای دسترسی مدیریت اطلاعات محرمانه احراز هویت کاربران از جمله مباحثی هستند که در این فصل مطرح و بعد از تبیین موضوع برای آن‌ها راهکار و دستورالعمل ارائه می‌شود
۱۰	رمزنگاری	نحوهٔ استفاده از کنترل‌های رمزنگاری و مدیریت کلید در این بخش عنوان می‌گردند
۱۱	امنیت محیطی و فیزیکی	در این فصل نحوهٔ امن کردن بخش‌ها، اتاق‌ها و تجهیزات، محافظت در برابر تهدیدات خارجی و محیطی، امنیت کابل کشی و نگهداری از تجهیزات توضیح داده می‌شود
۱۲	امنیت عملیات	در این بخش دستورالعمل‌هایی برای مستندسازی رویه‌های عملیات، مدیریت تغییر، مدیریت ظرفیت، جداسازی محیط‌های توسعه، تست و عملیات، نحوهٔ محافظت در برابر بدافزار، پشتیبان‌گیری از اطلاعات، ثبت گزارش وقایع و محافظت از آن‌ها، نصب نرم‌افزار روی سیستم‌های عملیاتی، مدیریت آسیب‌پذیری‌های فنی، محدودیت‌های مربوط به نصب نرم‌افزارو کنترل‌های ممیزی روی سیستم‌های اطلاعاتی ارائه می‌گردد
۱۳	امنیت ارتباطات	در این فصل به تبیین و تشریح دستورالعمل‌های مربوط به کنترل‌های شبکه، امنیت سرویس‌های شبکه، جداسازی در شبکه‌ها، سیاست‌ها و روال‌های انتقال اطلاعات، پیام‌رسانی الکترونیکی می پردازند
۱۴	مالکیت، توسعه و نگهداری سیستم	الزامات امنیتی سیستم‌های اطلاعاتی، امن کردن سرویس‌های کاربردی روی شبکه‌های عمومی، محافظت از داده‌های آزمون، امنیت در فرآیندهای توسعه و پشتیبانی در این بخش مطرح می‌شوند
۱۵	روابط تامین‌کننده	تعریف سیاست امنیت اطلاعات برای روابط تامین‌کننده و گنجاندن امنیت در قراردادها، ارائه دستورالعمل برای تعریف زنجیره تامین ارتباطات و اطلاعات، نظارت بر سرویس‌های تامین‌کننده و مدیریت تغییرات سرویس‌های تامین‌کننده از جمله مباحث مطرح شده در این فصل از استاندارد ایزو ۲۷۷۹۹ می‌باشند
۱۶	مدیریت حادثه در امنیت اطلاعات	تعریف مسئولیت‌ها و روال‌ها برای شرایط بروز حادثه در امنیت اطلاعات، تهیه گزارش برای رویدادهای مربوط به امنیت اطلاعات، تهیه گزارش دربارهٔ نقاط ضعف امنیت اطلاعات سازمان و جمع‌آوری شواهد از جمله اقداماتی است که باید یک سازمان بهداشتی-درمانی برای محافظت از تمامیت، محرمانگی و دسترسی‌پذیری اطلاعات پزشکی شخصی انجام دهد. این بخش به این موضوع و نحوهٔ انجام آن می پردازد.
۱۷	جنبه‌های امنیت اطلاعات از منظر مدیریت استمرار کسب‌وکار	برنامه‌ریزی، پیاده‌سازی تایید و بازبینی پیوستار امنیت اطلاعات در این بخش مطرح می‌شود
۱۸	انطباق	شناسایی الزامات قانونی و قراردادی قابل اجرا، قوانین مربوط به کنترل‌های رمزنگاری در این بخش مطرح می‌شوند
پیوست A		تهدیدات مربوط به امنیت اطلاعات پزشکی
پیوست B		طرح اقدام عملی برای اجرای ایزو ۲۷۰۰۲ در حوزهٔ بهداشت و درمان
پیوست C		بازبینه‌ای برای انطباق با ایزو ۲۷۷۹۹
کتابشناسی		استانداردهای مرتبط با امنیت اطلاعات پزشکی. جدول ۲ معرفی مختصری از استانداردهای ارائه شده در این بخش را ارائه می‌دهد.

جدول ۲: استانداردهای مرتبط با امنیت اطلاعات پزشکی

طبقه‌بندی استاندارد	نام استاندارد	عنوان
پیاده‌سازی گواهی‌نامه‌ها یا امضاهای دیجیتال در حوزهٔ سلامت	ISO 17090-1	انفورماتیک سلامت-زیرساخت کلید عمومی-بخش ۱: مروری بر سرویس‌های گواهی‌نامه دیجیتالی
	ISO 17090-2	انفورماتیک سلامت-زیرساخت کلید عمومی-بخش ۲: پروفایل گواهی‌نامه
	ISO 17090-3	انفورماتیک سلامت-زیرساخت کلید عمومی-بخش ۳: مدیریت خط مشی اعتبار گواهی‌نامه
حفظ امنیت اطلاعات پزشکی در مرزهای قضایی	ISO 22857	انفورماتیک سلامت-دستورالعمل‌های مرتبط با حفاظت داده‌ها برای تسهیل انتقال فرامرزی اطلاعات پزشکی شخصی
مدیریت امتیاز	ISO/TS 22600-1	انفورماتیک سلامت- مدیریت امتیاز و کنترل دسترسی- بخش ۱: مرور و مدیریت خط مشی
	ISO/TS 22600-2	انفورماتیک سلامت- مدیریت امتیاز و کنترل دسترسی- بخش ۲: مدل‌های رسمی
	ISO/TS 22600-3	انفورماتیک سلامت- مدیریت امتیاز و کنترل دسترسی- بخش ۳: پیاده‌سازی‌ها
	ISO/TS 21298	انفورماتیک سلامت- نقش های ساختاری و وظیفه ای
ناشناس یا مستعار کردن اطلاعات پزشکی شخصی	ISO/TS 25237	انفورماتیک سلامت- نام مستعار
سایر	ISO/TR18307	انفورماتیک سلامت- قابلیت همکاری و سازگاری در استانداردهای پیام‌رسانی و ارتباطات - ویژگی‌های اصلی
	ISO/TS 18308	انفورماتیک سلامت- نیازمندی‌های معماری رکورد الکترونیکی سلامت
	ISO/IEC 27001	فناوری اطلاعات- تکنیک‌های امنیت- سیستم‌های مدیریت امنیت اطلاعات-الزامات
	ISO/IEC15408-1	فناوری اطلاعات- تکنیک‌های امنیت- معیار ارزیابی امنیت فناوری اطلاعات- بخش ۱: معرفی و مدل عمومی
	ISO/IEC15408-2	فناوری اطلاعات- تکنیک‌های امنیت- معیار ارزیابی امنیت فناوری اطلاعات- بخش ۲: الزامات کارکردی امنیت
	ISO/IEC15408-3	فناوری اطلاعات- تکنیک‌های امنیت- معیار ارزیابی امنیت فناوری اطلاعات- بخش ۳: الزامات تضمین امنیت
	ISO/IEC 13335-1	فناوری اطلاعات- تکنیک‌های امنیت- مدیریت امنیت فناوری اطلاعات و ارتباطات- بخش ۱: مفاهیم و مدل‌های مدیریت امنیت فناوری اطلاعات و ارتباطات
	ISO/IEC TR 13335-3	فناوری اطلاعات- راهنمای مدیریت امنیت فناوری اطلاعات- بخش ۳: تکنیک‌های مدیریت امنیت فناوری اطلاعات
	ISO/IEC TR 13335-4	فناوری اطلاعات- راهنمای مدیریت امنیت فناوری اطلاعات- بخش ۴: انتخاب محافظ‌ها
	ISO/IEC TR 13335-5	فناوری اطلاعات- راهنمای مدیریت امنیت فناوری اطلاعات- بخش ۵: راهنمای مدیریت امنیت شبکه
	ISO/TR 20514	انفورماتیک سلامت- رکورد پزشکی الکترونیکی- تعریف، حوزه و محتوا
	HB 174:2003	مدیریت امنیت اطلاعات- دستورالعمل پیاده‌سازی برای بخش سلامت
	HB 231:2000	راهنمای مدیریت ریسک امنیت اطلاعات
	AS/NZS 4360	مدیریت ریسک
	JIP-ISMS-114-1.0	راهنمای کاربران ISMS برای سازمان‌های پزشکی- راهنمای استفاده از معیارهای صدور گواهی‌نامه ISMS
	ISO 7498-2	سیستم‌های پردازش اطلاعات- اتصال سیستم‌های باز- مدل مرجع پایه- بخش ۲: معماری امنیت
	ISO/IEC Guide 73	مدیریت ریسک-واژگان- دستورالعمل به‌کارگیری در استانداردها

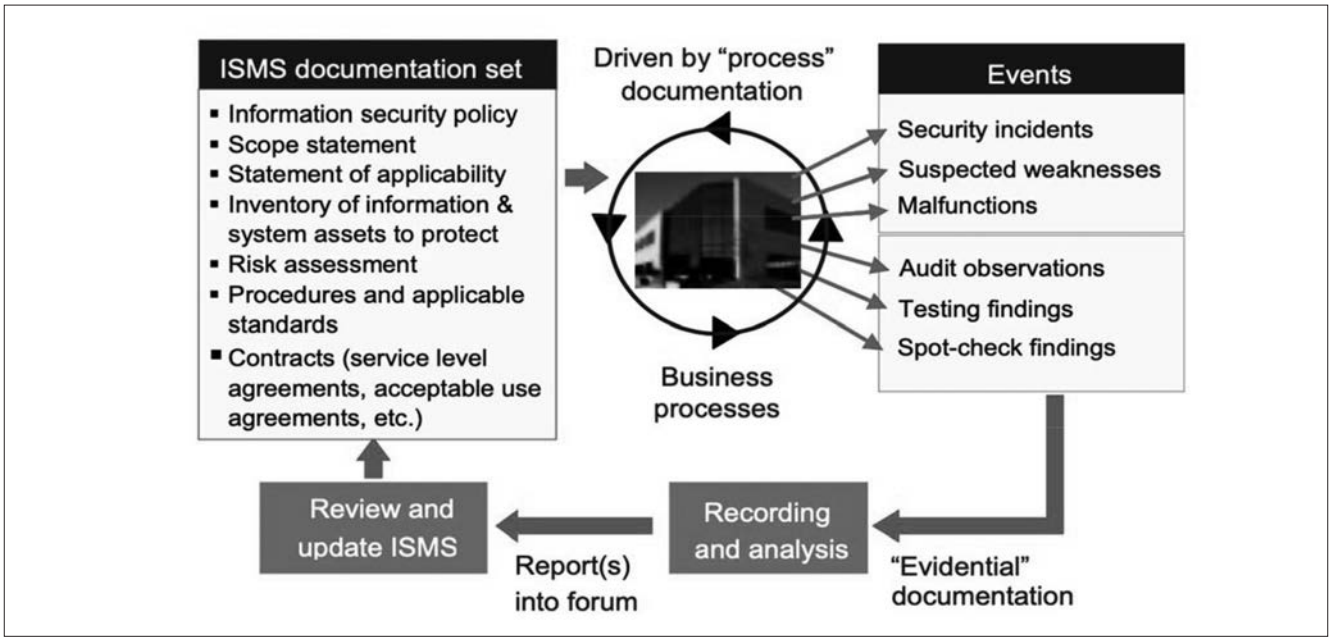
امنیت اطلاعات عبارت است از محافظت اطلاعات دربرابر طیف وسیعی از تهدیدات تا استمرار کسب‌وکار، به حداقل رساندن ریسک کسب‌وکار و به حداکثر رساندن بازگشت سرمایه و فرصت‌های تجاری تضمین شود.

امنیت اطلاعات از طریق اجرای مجموعه مناسبی از کنترل‌ها، شامل سیاست‌ها، فرآیندها، رویه‌ها، ساختارهای سازمانی و توابع نرم‌افزاری و سخت‌افزاری حاصل می‌شود. این کنترل‌ها باید هرجایی که لازم است مستقر و اجرا شده و مورد نظارت، بازبینی و بهبود قرار بگیرند تا برآوده شدن اهداف تجاری و امنیتی خاص سازمان تضمین گردد.

۳-۲- سیستم مدیریت امنیت اطلاعات

سیستم مدیریت امنیت اطلاعات (ISMS) یک چارچوب مدیریت جامع است که سازمان‌ها از طریق آن ریسک‌های اطلاعاتی خودش را شناسایی، تحلیل و اداره می‌کنند. سیستم مدیریت امنیت اطلاعات اطمینان می‌دهد که تنظیمات امنیتی به گونه‌ای تنظیم شده‌اند که می‌توانند با تغییرات در تهدیدات امنیتی، آسیب پذیری‌ها و تاثیرات تجارت همراه و همگام شوند.

اطلاعات پزشکی شخصی به‌صورت الکترونیکی در سیستم‌هایی ذخیره و بازیابی می‌شوند که به آن‌ها سیستم‌های اطلاعات پزشکی (HIS) گفته می‌شود. HIS یک مولفه جداناپذیر هر سیستم بهداشتی-درمانی



شکل ۱: سیستم مدیریت امنیت اطلاعات

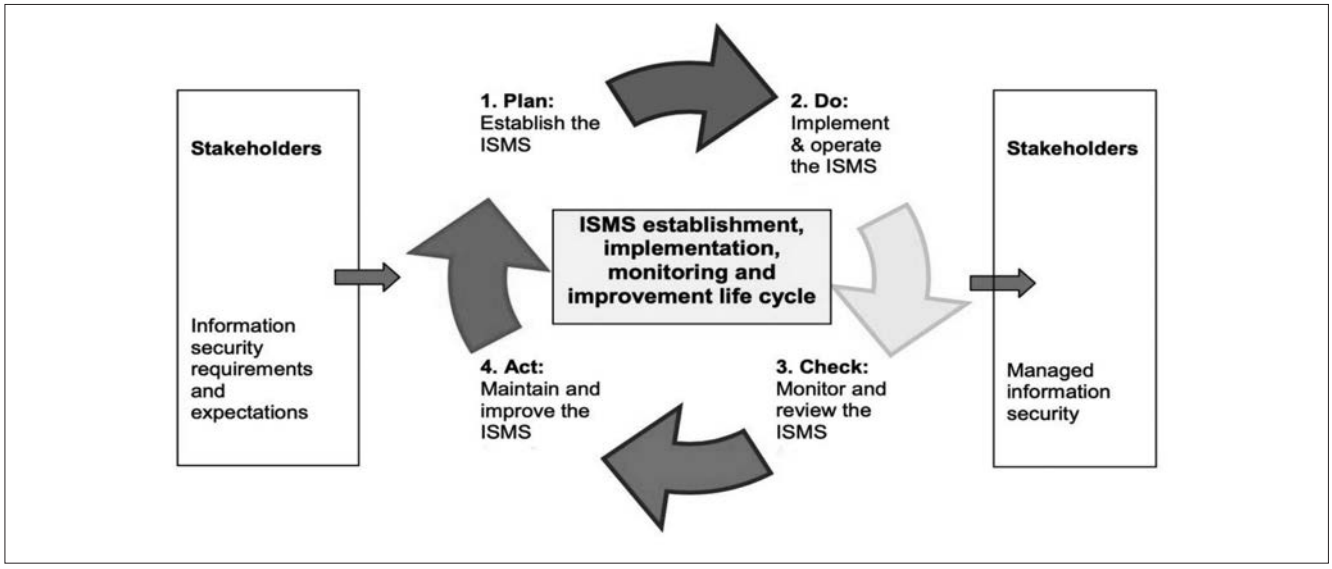
است. این سیستم‌ها امکان جمع‌آوری داده، پردازش و تحلیل اطلاعات پزشکی را فراهم نموده و توسعهٔ شاخص‌های مناسب برای نظارت و ارزیابی عملکرد سیستم بهداشتی-درمانی را تسهیل می‌کنند. این در حالی است که جمع‌آوری و ذخیره داده‌ها با استفاده از HIS می‌تواند مشکلات امنیتی به همراه داشته باشد؛ مشکلاتی که به‌طور معمول در روش کاغذی جمع‌آوری داده رخ نمی‌دهند. بنابراین سیستم‌های اطلاعات پزشکی باید مدیریت مناسبی از نقطه نظر امنیت اطلاعات داشته.

ایزو ۲۷۰۰۱ مفهوم ISMS را معرفی می‌کند و توضیح می‌دهد که تحقق اهداف امنیتی نیازمند این چارچوب کنترلی است. استاندارد ایزو ۲۷۰۰۲ – کد عملی برای -ISMS پیاده‌سازی استاندارد ایزو ۲۷۰۰۱ را پشتیبانی نموده و برای اجرای کنترل‌های امنیتی ارائه شده در استاندارد ایزو ۲۷۰۰۱ دستورالعمل ارائه می‌دهد. تجربه بین‌المللی و اصول بهروش‌های شناخته شده در حوزهٔ امنیت اطلاعات نشان می‌دهند که از طریق پیاده‌سازی یک سیستم مدیریت مانند آنچه در شکل ۱ نشان داده شده است، می‌توان به بهترین وجه از انطباق مداوم با ایزو ۲۷۰۰۲ اطمینان حاصل کرد. در سال ۲۰۰۸ یک استاندارد جدید برای مدیریت امنیت اطلاعات در حوزهٔ سلامت منتشر شد. استاندارد بین‌المللی ایزو ۲۷۷۹۹ برای سازمان‌های بهداشتی-درمانی و سایر متولیان اطلاعات پزشکی دستورالعمل‌هایی ارائه می‌دهد که به کمک آن‌ها بتوانند استاندارد ایزو ۲۷۰۰۲ را اجرا نموده و بهترین مراقبت از محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات خود را فراهم نمایند.

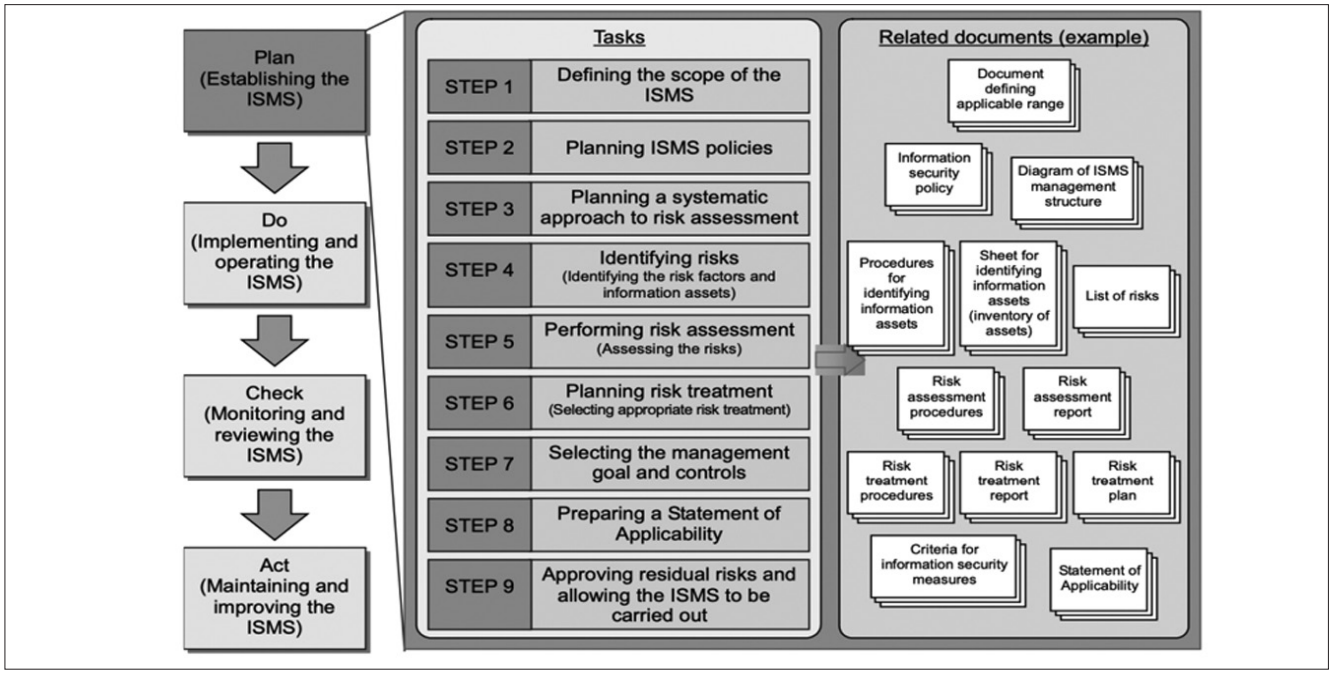
همان‌طور که در شکل ۲ نشان داده شده است، پیاده‌سازی یک ISMS نیازمند دنبال کردن چرخه‌ای از فعالیت‌هاست و به ۴ فاز تقسیم می‌شود: Check، Do، Plan و Act. به این فرآیندها مدل PDCA گفته می‌شود. استاندارد ایزو ۲۷۰۰۱ از این رویکرد (یا چرخه)، که برای تشکیل تمام فرآیندهای ISMS و الزامات مربوط به بهبود مداوم اعمال می‌شود استفاده می‌کند.

شکل‌های ۳ تا ۶ وظایف و مستندات مرتبط با هریک از مراحل فوق را نشان می‌دهند. از لحاظ نظری، ایزو ۲۷۰۰۲ روی کل سازمان قابل اعمال است. اما تجربیات حاصل از پیاده‌سازی آن در انگلستان نشان داده است که واحدهای بسیار بزرگ برای تکمیل کار مورد نظر و تحویل سطح انطباق مورد نیاز با مشکل مواجه می‌شوند. بنابراین اولین کار در مرحله برنامه‌ریزی یا همان Plan، تعیین محدودهٔ انطباق است. ثابت شده است که محدوده انطباقی که بیش از ۲ یا ۳ مکان (تقریبا ۵۰ پرسنل یا ۱۰ فرآیند) را پوشش نمی‌دهد بسیار خوب کار می‌کند. بعد از انتخاب و تعریف محدوده انطباق، نوبت به تحلیل شکاف می‌رسد. در تحلیل شکاف ارزیابی سطح بالایی از انطباق انجام می‌شود. بهروش‌ها نشان داده‌اند که این تحلیل باید روی مسئولیت سازمانی، پیاده‌سازی، مستندات مربوط به اقدامات امنیتی و مدارک مورداستفاده در تحلیل متمرکز باشد. در مرکز یک ISMS نظرگاه مدیریت امنیت اطلاعات (ISMF) قرار دارد و ایجاد یک ISMF مناسب از جمله کارهای کلیدی است که در مرحله برنامه‌ریزی انجام می‌گیرد. وظیفه این نظرگاه هدایت و نظارت بر امنیت اطلاعات است. ارزیابی خطراتی که اطلاعات پزشکی را تهدید می‌کنند، مدیریت ریسک، برنامه‌ریزی بهبود امنیت، بیانیه کاربردپذیری و تنظیم سند ISMS از جمله کارهای دیگری هستند که در این مرحله باید انجام شوند.

پیاده‌سازی ISMS از مراحل زیر تشکیل شده است:



شکل ۲: فرآیند ISMS

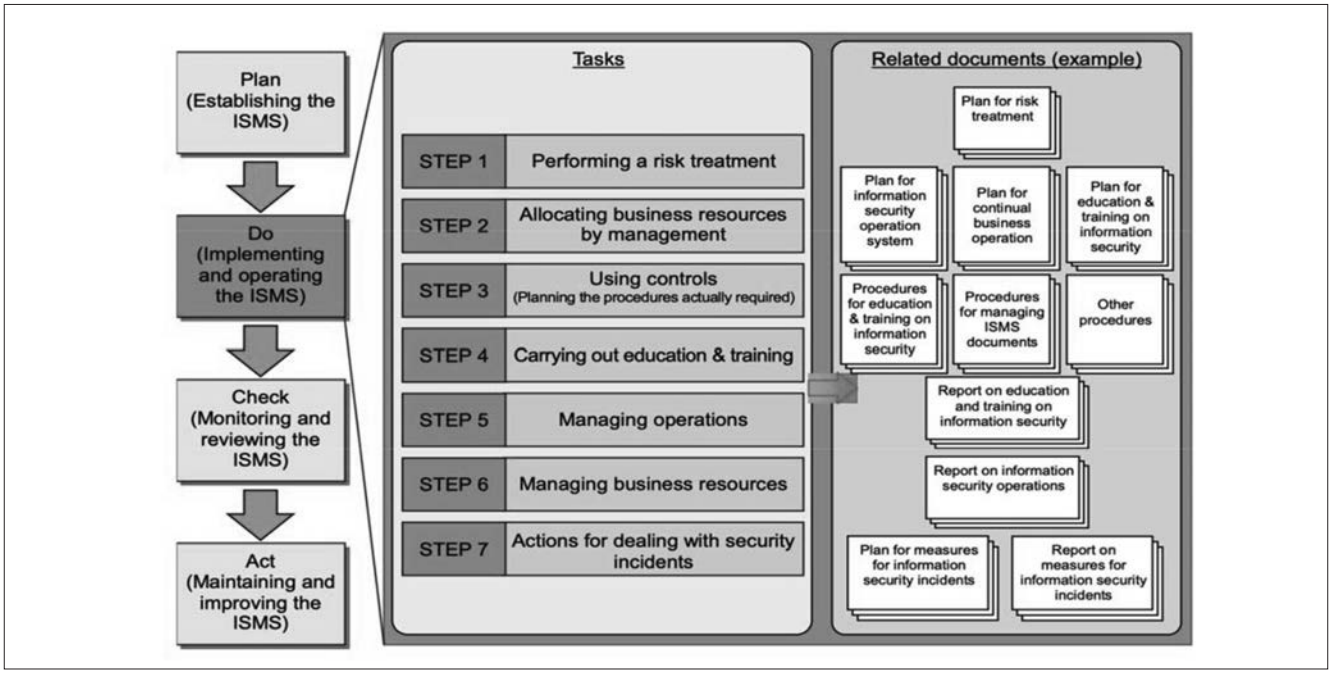


شکل ۳: وظایف و اسناد مرتبط با استقرار ISMS (فاز Plan)

۱- ایجاد طرح مواجه با ریسک
۲- تخصیص منابع
۳- انتخاب و اجرای کنترل‌های امنیتی
۴- آموزش
۵- مدیریت عملیات
۶- مدیریت منابع
۷- مدیریت رویدادهای امنیتی

سازمان، ISMS و در درون آن ISMF باید از اثربخشی خود هم در حفظ سطح امنیت فعلی و همچنین در بهبود مستمر در راستای استراتژی امنیت اطلاعات و مطابق با اهداف سازمان اطمینان داشته باشند. برای حصول این اطمینان گزینه‌های متعددی وجود دارد. سازمان‌های بهداشتی-درمانی باید برنامه‌های حسابرسی و ممیزی سازگاری ایجاد کنند. لازم است این برنامه‌ها ترکیبی از فناوری‌ها و رویکردها را مورداستفاده قرار دهند. کسب این تضمین مستمر، ارزیابی سازگاری در سه سطح خودارزیابی، بررسی دقیق و بازرسی مستقل، کسب گواهی‌نامه ایزو ۲۷۰۰۱ از جمله فعالیت‌هایی هستند که در مرحله بررسی انجام می‌گیرند.

نتایج فعالیت‌های نظارت که در مرحلهٔ بررسی انجام می‌گیرند برای



شکل ۴: وظایف و اسناد مرتبط با پیاده‌سازی و اجرای ISMS (فاز Do)

بررسی بیشتر به ISMF داده می‌شوند، چرا که این ISMF است که مسئول تصحیح نواقص و حفظ اثربخشی عملیاتی ISMS می‌باشد و این فعالیت مهمی است که در فاز Acting انجام می‌شود.

۳-۳- اطلاعاتی که در حوزهٔ سلامت نیاز به محافظت دارند

چندین نوع اطلاعات وجود دارد که لازم است محرمانگی، یکپارچگی و دسترسی‌پذیری آن‌ها حفظ و مراقبت شود:

۱- اطلاعات پزشکی شخصی

۲- داده‌های مستعاری که از اطلاعات پزشکی شخصی و به واسطه برخی از متدولوژی‌های شناسایی مستعارها استخراج می‌شوند.

۳- داده‌های آماری و پژوهشی، شامل داده‌های ناشناسی که از اطلاعات پزشکی شخصی و از طریق حذف داده‌های هویتی شخصی به دست می آیند.

۴- دانش پزشکی-بالینی که هیچ یک از موضوعات خاص مراقبت مربوط نیستند، شامل داده‌های بالینی پشتیبانی از تصمیم (مثل داده‌های مربوط به واکنش‌های دارویی نامطلوب)

۵- داده‌های مربوط به متخصصین حوزه سلامت، پرسنل و نیروهای داوطلب

۶- اطلاعات مرتبط با نظارت بر بهداشت عمومی

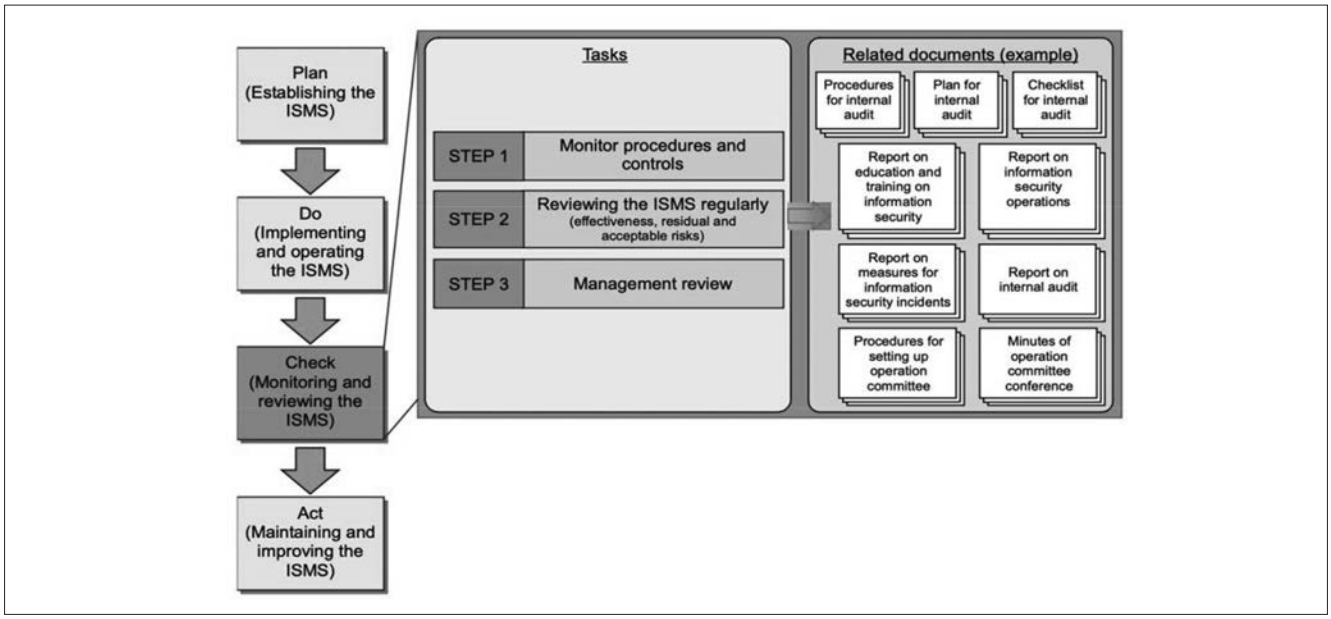
۷- داده‌های دنباله حسابرسی که توسط سیستم‌های اطلاعاتی پزشکی تولید شده و حاوی اطلاعات پزشکی شخصی، داده‌های مستعار مستخرج از اطلاعات پزشکی شخصی و یا داده‌های مربوط به اقدامات کاربران روی اطلاعات پزشکی شخصی می‌باشند.

۸- داده‌های امنیت سیستم برای سیستم‌های اطلاعاتی پزشکی شامل داده‌های کنترل دسترسی، داده‌های پیکربندی امنیت سیستم

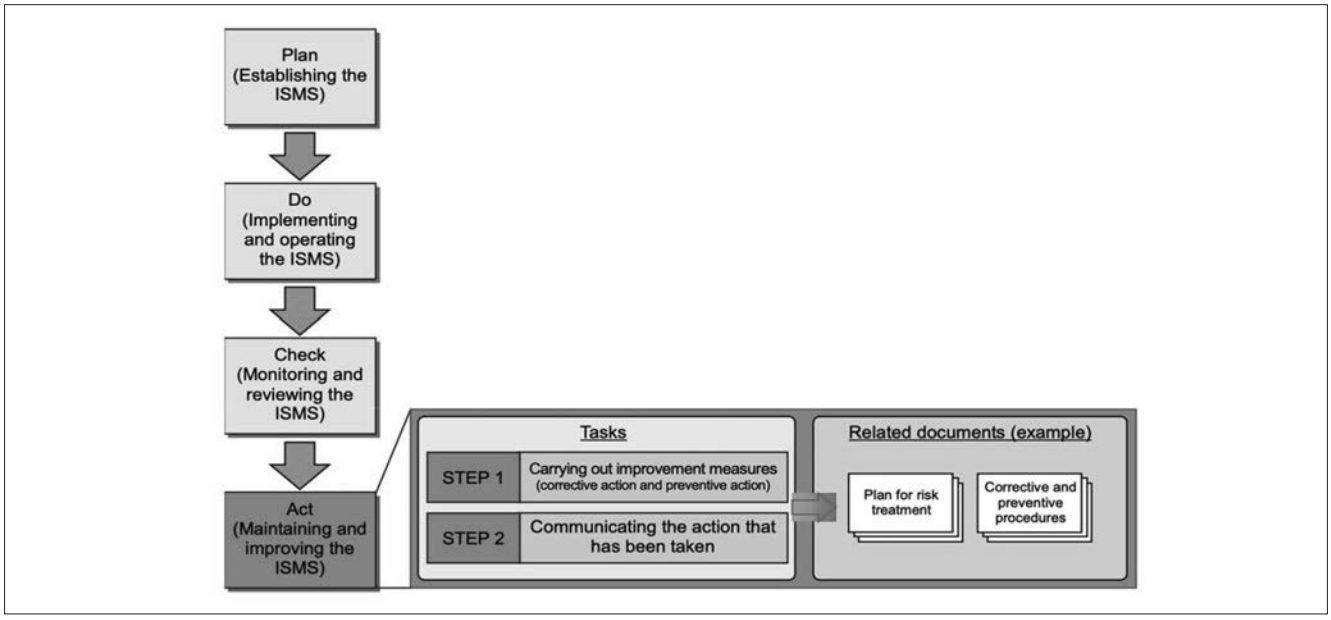
میزان محافظت از محرمانگی، یکپارچگی و دسترسی‌پذیری به ماهیت اطلاعات، مورد استفاده اطلاعات و ریسک‌هایی که اطلاعات با آن‌ها مواجه هستند بستگی دارد. به‌عنوان مثال داده‌های آماری (مورد ۳ از فهرست فوق) ممکن است محرمانه نباشند اما حفظ یکپارچگی آن‌ها می‌تواند بسیار مهم باشد. به همین ترتیب داده‌های دنباله حسابرسی (مورد ۷ در فهرست فوق) ممکن است به دسترسی‌پذیری بالایی نیاز نداشته باشند (بایگانی کردن مکرر و با یک زمان بازیابی در مقیاس ساعت به جای ثانیه، می‌تواند برای یک برنامه کاربردی خاص کافی باشد) اما ممکن است محتوای آن به شدت محرمانه باشد. ارزیابی ریسک می‌تواند سطح موردنیاز برای محافظت از محرمانگی، یکپارچگی و دسترسی‌پذیری را به شکل مناسبی تعیین نماید. نتایج ارزیابی منظم ریسک باید با اولویت ها و منابع سازمان مجر متناسب باشد.

۳-۴- تهدیدات و آسیب‌پذیری‌ها در امنیت اطلاعات پزشکی

تهدیدات و آسیب‌پذیری‌های امنیت اطلاعات در حوزهٔ سلامت بسیار متنوع هستند. با وجود این که هیچ کدام از این تهدیدات و آسیب‌پذیری‌ها منحصر به بهداشت و درمان نیستند اما این حوزه فاکتورهایی دارد که باید هنگام ارزیابی تهدیدات و آسیب‌پذیری‌ها در نظر گرفته شوند و همین باعث منحصر به فرد شدن بخش سلامت می‌شود. - سازمان‌های بهداشتی-درمانی براساس ماهیتشان در محیطی فعالیت می‌کنند که ممکن است هیچ گاه نتوان بازدیدکنندگان و عموم مردم را از آن مستثنی کرد. در سازمان‌های بهداشتی-درمانی بزرگ میزان دقیق افرادی که در نواحی عملیاتی این سازمان‌ها تردد می‌کنند رقم قابل تجهی است.



شکل ۵: وظایف و اسناد مرتبط با نظارت و بازبینی ISMS (مرحلهٔ بررسی)



شکل ۶: وظایف و اسناد مرتبط با بهبود ISMS (مرحلهٔ اقدام)

این مسئله آسیب‌پذیری سیستم‌ها در برابر تهدیدات فیزیکی را افزایش می‌دهد و هنگامی که پای بیماران مبتلا به بیماری‌های ذهنی یا عاطفی در میان باشد احتمال وقوع این تهدیدات بیشتر هم می‌شود.

اهمیت حیاتی شناسایی موضوع تحت مراقبت و مطابقت دادن صحیح آن با رکوردهای پزشکی‌اش، سازمان بهداشتی-درمانی را به سمت جمع‌آوری اطلاعات هویتی دقیق سوق می‌دهد. دفاتر منطقه‌ای یا قضایی بیماران (دفاتر ثبت بیماران) گاهی جامع‌ترین و به روزترین مخازن اطلاعات هویتی در یک محدودهٔ قضایی هستند. این اطلاعات هویتی ارزش بالقوه بزرگی برای کسانی هستند که از این اطلاعات برای سرقت هویت استفاده می‌کنند و بنابراین باید با دقت بسیار زیادی محافظت شوند.

بسیاری از سازمان‌های بهداشتی-درمانی به‌طور مزمن با کمبود بودجه مواجه هستند و پرسنل آن‌ها گاهی موظف هستند تحت استرس قابل توجهی و با سیستم‌هایی که باید تا مدت‌ها پس از بازنشستگی آن‌ها آماده سرویس‌دهی باشند کار کنند.

این فاکتورها می‌توانند پتانسیل انواع خاصی از تهدید را افزایش داده و آسیب‌پذیری‌ها را تشدید کنند. از سوی دیگر، مراقبت بالینی طیفی از پرسنل، متخصص،نیروی فنی، اجرایی، کمکی و داوطلب را در بر می‌گیرد. فداکاری و تنوع تجربه گاهی باعث کاهش آسیب‌پذیری

می‌شـود. آموزش حرفه‌ای سـطح بالایی که اکثـر متخصصین حوزه سلامت دریافت می‌کنند نیز باعث کاهش وقوع تهدیدات داخلی شده و بهداشت و درمان را از سایر بخش‌های صنعتی جدا می‌سازد.
بنابرایـن محیط بهداشـتی-درمانی با تهدیدات و آسـیب‌پذیری‌های منحصر به فرد خود باید مورد توجه خاص قرار بگیرد.
ایزو ۲۷۷۹۹ در پیوست A فهرستی از انواع تهدیداتی را ارائه می‌دهد که لازم است هنگام ارزیابی خطرات مرتبط با محرمانگی، یکپارچگی و دسترسی‌پذیری اطلاعات پزشـکی و یکپارچگی و دسترسی‌پذیری سیسـتم‌های اطلاعاتی مرتبط مورد توجه سـازمان‌های بهداشـتی-درمانی قرار بگیرد.

۴- خلاصه

اسـتاندارد ایزو ۲۷۰۰۱ در تمام سـازمان‌های تجـاری و دولتی دنیا به‌عنوان پایه و اسـاس مدیریت سیاست سازمان و پیاده‌سازی امنیت اطلاعات مورد اسـتفاده قرار می‌گیرد. از آن جایی که این اسـتاندارد به گونه‌ای منعطف طراحی شـده اسـت می توان از آن در تمام انواع سازمان‌ها استفاده کرد و از این رو به‌صورت بالفعل به «زبان مشترک» سیسـتم‌های مدیریت امنیت اطلاعات تبدیل شـده است. با توجه به کلـی بودن اسـتاندارد ایـزو ۲۷۰۰۱ و منحصربه فـرد بودن محیط عملیاتی سازمان‌های بهداشتی-درمانی، پیاده‌سازی این استاندارد در این سـازمان‌ها نیازمند دستورالعمل و کارهای طراحی و تحلیل داده بسـیار زیادی است. استاندارد ایزو ۲۷۷۹۹ در واقع یک نمونهٔ تکمیل شـده از اسـتانداردهای کلی ایـزو ۲۷۰۰۱ و ۲۷۰۰۲ بوده و آن‌ها را خاص صنعت بهداشـت و درمـان تعریف می‌کند. علـت این امر نیز این اسـت که این اسـتانداردهای کلی در بطن یک حوزهٔ خاص مورد بحـث قرار نگرفتـه و از این رو اغلب اوقات بی‌فایده تلقی می‌شـوند. به‌عبـارت دیگر اسـتقرار ISMSهای کارا و موثـر در این محیط‌ها به دسـتورالعمل‌های اضافی نیاز دارند. اگر این رهنمودهای اضافی ارائه نشوند ممکن است پیامدهای نامطلوبی به دنبال داشته باشد. به‌عنوان مثال اگر ارزیابی ریسـک امنیت اطلاعات برای تضمین اجرای مداوم و بدون وقفه سـرویس‌های اضطراری مرتبط بـا مدیریت یک فاجعه کنترل‌هایی را در نظر نگیرد، مرکز درمانی هنگام نیاز به ارائه این‌گونه سـرویس‌ها ناکارآمد خواهد بود و این می‌تواند به از دسـت رفتن یک زندگی منجر شـود. واقعیت محیط‌های بهداشـتی-درمانی این است که طراحی و پیاده‌سـازی ISMS اهمیت ویژه‌ای دارد. استاندارد ایزو ۲۷۷۹۹ که نسـخه اسـتاندارد ایـزو ۲۷۰۰۱ و ۲۷۰۰۲ برای مراکز درمانی اسـت، این موضوع را محقق سـاخته و به تفسیر مناسب این استانداردها در یک زمینه عملیاتی خاص کمک می‌کند.
در این نوشـتار سعی شد معرفی مختصری از استاندارد ایزو ۲۷۷۹۹، ارتباط آن با سایر استانداردهای ایزو و مخصوصا خانواده ۲۷k و نحوهٔ استفاده از آن در یک سازمان بهداشتی-درمانی مورد مطالعه و بررسی قرار بگیرد.

۵- منابع

[1] https://www.iso.org/standard/62777.html
[2] S. Tyali, D. Pottas.” Information Security Management Systems in the Healthcare Context”. Proceedings of the South African Information Security Multi-Conference (SAISMC 2010)
[3] https://www.iso.org/about-us.html

آلن تورینگ و اقتصاد دانش‌بنیان در عصر کرونا: زندگی پنهان ذهن، یادگیری ژرف و وب معنایی در مواجهه با بایگانی همیشگی اسنودن

سید ابراهیم ابطحی
استادیار دانشکده مهندسی کامپیوتر- دانشگاه صنعتی شریف
نایب رئیس انجمن انفورماتیک ایران
پست الکترونیکی: abtahi@sharif.edu

پیش گفتار

حـالا که کووید ۱۹ در شـمایل کرونا، فنـاوری اطلاعات و متعلقات وابسـته و پیوسـته آن را، به سـطح منجی، بابت فراهم‌سازی امکان دورکاری، در قرنطینـه جهانـی (که بـه قولی تجربـه جهانی زندان انفرادی اسـت) ارتقاء داده، در اوج قدرت و محبوبیت آن، جوانمردانه می‌شـود بر آن شورید. می‌شـود حق را به وایزن بوم[1] داد که علیرغم شـراکت در ابداع هوش مصنوعی با نرم‌افزار الیزا[2] در تقابل دیدگاهی بـا برخی از همکاران خـود نظیر ماروین مینسـکی[3]، آینده‌نگارانه از کارشناسـان رایانه بپرسـد: آیا همچون پدران بمب اتم خود بد آوازه نخواهند شد؟ (قریب به این مضمون در نوشته‌ای). اما تعجب‌آور است که گذشـته بین آینده‌نگاری چون نوح هراری[4]، در جایگاه شخصیتی رسـانه‌ای با مسـامحه‌ای بعید، از نقد فناوری‌های شکل گرفته بر پایه نیازآفرینی و نه برحسـب نیـاز، بگریزد و به مثال عـوام‌زدۀ قیاس با چاقو، در امکان کشـتن یا پوسـت کندن سـیب، متوسل شود. یعنی حتـی در حد کرانبرگ هم به تهدیدهای فناوری‌های لجام گسـیختۀ همگرا (که شـزان[5] می‌نامندش) اشـاره نکند[6]. آیا امروز، برخی دچار عوام زدگی فناورانه شده‌اند؟ تجارت که حیات را به معاش تقلیل داده و با پتک رسانه‌ای، موفق شده است برخی را قانع کند، که با فراموشی وظایـف غیر لویاتانی مدیران، خیر عام آنسـت که سـلامت در مذبح اقتصاد هزینۀ رونق شود، تا خیل روزمره زیستان، از گرسنگی نشورند. عجیب‌تر آن است، که قریب به این مضمون را از منظری دیگر از زبان فیلسوف اخلاقی چون پل سینگر[7] بشنوید[8] و به تحلیل‌های خلاف آن شـک کنید که خوشبختانه تحلیل فیلسـوف سیاسی مایکل سندل[9] شـما را منصرف می‌کند[10]. آنچه زندگی پساکرونایی می‌نامند با مجوز سیاست اقتضایی، آینده‌ای به‌نظر می‌رسد در حسرتخواری گذشته، یا ناکجا آبادی، در سیمای بهشتی فناورانه، که می‌اندیشد شاید بد نباشد نگرانی‌هایش از ارتباطات انسانی نفس به نفس دردسر ساز را با جهان مجـازی کنترل پذیر و آواتارهای خیالـی اش جایگزین کند (۱۹۸۴

1- Weizenbaum, Josef

۲-ELIZA از اولین برنامه‌های هوش مصنوعی برای پردازش زبان طبیعی

3-Marvin Minsky

4-Yuval Noah Harari

۵- شزان (شناختی + زیستی + اطلاعاتی + نانو: (NBIC: Nano+Bio+It+Cognative

۶- کرانبرگی که گفت: فناوری نه خوب است و نه بد ، اما قطعا خنثی نیست.

7- Peter Singer

۸- پیتر سـینگر، «چه زمانـی درمان پاندمی از خود بیماری بدتر خواهد بود؟ (همه چیز در سـلامتی خلاصه نمی‌شود)»، ماهنامه اندیشه پویا، شماره ۶۶، اردیبهشت ۱۳۹۹.

9- Michael Sandel

۱۰- تومـاس ال.فریدمـن، «یافتـن خیـر عمومـی در پاندمی»، گفتگو با مایکل سـندل فیلسـوف سیاسـی دانشگاه‌هاروارد، ماهنامه اندیشه پویا، شماره ۶۶،خرداد۱۳۹۹.

در ۲۰۲۰؟). شـرایطی که به روایت اسـنودن[11] در بایگانی همیشگی، نمی‌شود نسبت به آن بی‌تفاوت بود، چرا که طعم ساده‌اندیشی دارد. به این بهانه گشتی می‌زنیم بین کتاب‌هائی که گونه‌های کاغذی آن‌ها را باید روزها، برای کوویدزدائی، پشـت در گذاشت و یا برای خواندن با گونه‌هـای الکترونیکی آن کش و قوس رفت و پس از خواندن چند برگ با چشـم‌های خسته ازخیرش گذشـت. در این شماره هم شش کتاب در موضوعات کما بیش مرتبط با این مقدمه را معرفی می‌کنیم.

عنوان کتاب: آلن تورینگ و پایه‌گذاری کامپیوترهای امروزی.
نویسنده: نایجل کاوتورن.
مترجم: امیرطاهر محسنی.
ناشر: نشر دیبایه.
زمان نشر: ۱۳۹۸.
تعداد صفحات: ۱۶۴ برگ.
شمارگان: ۵۰۰نسخه.
شابک: ۹۷۸-۶۰۰-۲۱۲-۳۷۲-۵.
قیمت: ۲۴۰۰۰ تومان.

مقدمه

کتاب کاوتورن همکار تورینگ در معرفی این نابغه عالم رایانه، خواندنی است زیرا سرنوشت انسـان توانمندی را با همه قوت‌ها وضعف‌هایش، با یک ابداع درخشان (ثمره عقل یا مغز) و عاقبتی دلخراش (ثمره تن ناساز و نابهنجار) بیان می‌کند و عواقب افشا کردن صادقانه - پیش از مجاز شـدن - موقعیتی ناخواسته را بیطرفانه تصویر می‌کند. زندگی، نبوغ و مرگ دگراندیشـی دگرباش، که مـرگ اتفاقی و ناباورانه او، از خودکشی تا قتل مدعی دارد. از منظری تقدیرگرا او را می‌توان، قربانی سرنوشت ناخواسته‌اش شمرد. کسی که بزرگ‌ترین جایزه علمی جهان رایانه به نام اوست و اقداماتش و ابداعاتش به گفته‌ای به دو سال زودتر تمام شدن بزرگ‌ترین جنگ جهانی انجامید.

محتوای کتاب

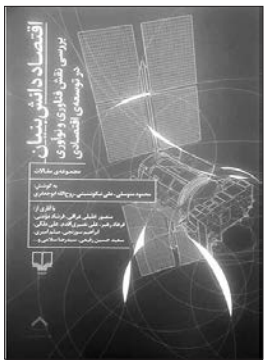
نویسـنده کتاب که دوسـت و همکار تورینگ بـوده در پایان کتاب نوشته است: «آلن تورینگ یکی از چهره‌های برجسته قرن است. نتایج کار او همه جا هست و کسی در حال حاضر نمی‌داند که ما را به کجا خواهد برد. جهان کامپیوتر و حالا جهان اینترنت ریشـه در ایده‌های بنیادین تورینگ دارند».

کتاب سـاختار سـاده‌ای دارد امـا نظیر زندگی نبشـته‌های متعارف نیسـت و با سیر اتفاقات زمانه تورینگ و تحولات زندگی او آن چنان در هم تنیده اسـت که گاه جنبه ادبی دل‌چسبی در حد رمانی کوتاه می‌یابد. خدمتی که نایجل به شکل ضمنی به دوست خود آلن در این نوشـته می‌کند، ترسیم ملاحظاتی اسـت که یک خدمتگزار به میهن و گاه مردمـی انبوه در جهان را، در حد یک قربانی، به خودکشـی یا دیگرکشـی توسط غیر می‌کشـد. نابغه‌ای که نیم قرن پس از مرگش، خدمات جهان شمولش، به رسمیت شناخته شد. او که هر واژه مرتبط با او بازنمائی کننده خدمتی است سترگ، واژه‌هائی نظیر رمزگشایی، انیگما، ماشین تورینگ و هوش مصنوعی.

در دسـامبر ۲۰۱۱ درخواسـت عفو تورینگ بابت تخلـف از قانونی ناموجود در زمان وقوع (دگرباشی مجاز)، ابتدا با مخالفت دولت مواجه شـد و تنها بـا تهیه لایحه عفـو در مجلس اعیان، نظـر دولت تغییر کـرد. امـا عاقبت در ۲۴ دسـامبر ۲۰۱۳، ملکه با اسـتفاده از قدرت قانونی ویژه خود برای بخشـش، عفونامه را امضا کرد. بلافاصله برخی شخصیت‌ها خواستار تحقیق در باره مرگ تورینگ شدند. نویسنده در اینجا می‌نویسـد: «ای کاش می‌شد هرگونه شکی در باره علت واقعی مرگ – تورینگ – بر طرف شـود، از جمله حدس و گمان‌هایی مبنی بر این‌که او را سازمان‌های امنیتی به قتل رسانده‌اند».

کتـاب دارای فهرسـت، پیش گفتاری با عنوان کشـف مهم در پارک بلچی[12]، نه فصل مطلب و منابعی برای مطالعه بیشـتر اسـت. عناوین فصول کتاب به شرح زیر است:

فصل ۱: تولد یک نابغه.
فصل ۲: تازه‌ترین یافته‌های ریاضیات.
فصل ۳: ذهن‌های حسابگر.
فصل ۴: انیگما.
فصل ۵: تغییرات انیگما.
فصل ۶: تولد کامپیوتر.
فصل ۷: آدم‌ها و ماشین‌ها.
فصل ۸: سیب سمّی.
فصل ۹: میراث تورینگ.



عنـوان کتـاب: اقتصـاد دانش‌بنیـان – بررسـی نقش فنـاوری و نوآوری در توسعهٔ اقتصادی.
مقالاتی از: منصورخلیلی عراقی، فرشاد مومنی و....
به کوشش: محمود متوسلی، علی نیکو نسبتی و روح‌الله ابوجعفری.
ناشر: نشر چشمه.
زمان نشر: ۱۳۹۵.
تعداد صفحات: ۲۳۸ برگ.
شمارگان: ۱۰۰۰ نسخه.
شابک: ۹۷۸-۶۰۰-۲۲۹-۶۶۸-۵.
قیمت: ۱۸۰۰۰ تومان.

11- Edward Joseph Snowden

۱۲- پارکی در ایالت باکینگهامشـر که مرکز تیم بریتانیائی عملیات شکسـتن رمز در جنگ جهانی دوم بود که در سال ۲۰۰۵ پس از بازسازی موزه ملی کامپیوتر را هم در خود جای داد.

مقدمه

ناشـر در پشت جلد کتاب نوشته اسـت: «بررسی سرفصل‌های مهم توسـعه از از نگاه رویکردهای مختلف موجب بهبود تبیین مسـائل و ارائهٔ توصیه‌های سیاسی مناسـب‌تر می‌شود. وجه تمایز این کتاب، با سـایر آثار در این حوزه، آن اسـت که علاوه بر بررسی مباحث اقتصاد دانش‌بنیـان و نـوآوری، که از جدی‌ترین موضوعات توسـعه در حال حاضر هسـتند، خوانندگانی به کمک آن می‌توانند آشـنایی اجمالی بـا مکاتب مختلف اقتصادی پیدا کنند. در واقع کتاب حاضر اولین اثر فارسـی است که در آن یک مسـئله از زاویهٔ دید طیف گسترده‌ای از مکاتب بررسی شده است.

در مجموعه توسـعه و اندیشـه که کتاب حاضر دومین اثر آن است، تلاش خواهد شـد مکاتب مختلف اقتصادی از جمله اتریشی، نهادی، مارکسیسـتی، شناختی و رفتاری معرفی شود و مورد بحث قرار گیرد و موضوعات مختلفی مانند عدالت، آزادی، توسعه، کار آفرینی، اقتصاد دانش محور، مباحث بازار پول و سرمایه، نقش دولت در توسعه و غیره از نگاه این مکاتب بررسی شود.

محتوای کتاب

کتاب دارای فهرسـت مطالب، دیباچـه، مقدمه، مقدمه مترجم، هفت مقاله، معرفی برخی از مراکز فعال در زمینهٔ دانش و فناوری در ایران و واژه نامه است.عناوین مقالات کتاب به شرح زیر است:

مقاله ۱: مروری بر رویکردها و نظریه‌های اقتصاد دانش‌بنیان.
مقالـه ۲: اقتصاد دانش‌بنیان: تعاریف، شـاخص‌ها، نقـش دولت‌ها و دلالت‌های آن برای ایران.
مقاله ۳: رویکرد اتریشی به اقتصاد دانش‌بنیان.
مقاله ۴: رویکرد نهادی به اقتصاد دانش‌بنیان.
مقالـه ۵: رویکرد تطـوری و اقتصاد دانش‌بنیان (بـا تمرکز بر برخی مفاهیم و دلالت‌ها).
مقاله ۶: بررسی ظرفیت قوانین ایران برای الگوبرداری از سیاست‌های همپایی صنعتی در کشورهای موفق.
مقاله ۷: آیا اقتصادهای نفتی می‌توانند دانش‌بنیان شوند؟ (چگونه؟).

عنوان کتاب: زندگی پنهان ذهن.
مولف: ماریانو سیگمان.
ناشر: نشر نو.
زمان نشر: چاپ اول ۱۳۹۸.
تعداد صفحات: ۳۲۷ برگ.
شمارگان: ۱۱۰۰ نسخه.
شابک: ۹۷۸-۶۰۰-۴۹۰-۰۶۴-۰۵.
قیمت: ۵۶۰۰۰ تومان.

مقدمه

استانیسـلانس دوان[۱۳] در باره این کتاب نوشته است: اگر طبق آنچه امیلی دیکینسـن نوشته مغز عمیق‌تر از دریا باشد، آنگاه کتاب ماریانو سـیگمان راهنمایی اسـت عالی بر ورطه‌های کشـف ناشدهٔ مغز. این کتاب پرمغز و در عین حال مختصر، سرشـار اسـت از اسـتعاره‌هایی روشـنگر. همراه این کتاب به سـفری بس سرگرم‌کننده، به ظرایف و عجایب ذهن انسـان می‌رویم. در طی این سفر به بینش‌هائی در مورد مفاهیم ناآشـنائی همچون «نبردهای ناآگاهانه درونی»، «خواب‌های واضح»، «مغزهای دو زبانه»، «نوزادانی که ذهن را می‌خوانند» دسـت می‌یابیم. همراه با متفکرانی برجسـته همچون چامسـکی، تورینگ، روسـو، افلاطون، سـی گـن و فروید برخـی نظرهایشـان را در پرتو آزمایش‌های هوشـمندانه سیگمان نظاره می‌کنیم. خواندن این کتاب از آغاز تا پایان بی‌اندازه لذت‌بخش اسـت: کتابی علمی و هیجان‌انگیز و مجذوب کننده.

راما چاندران[۱۴] درباره این کتاب نوشـته اسـت: ماریانو سیگمان ما را به سـفری باشکوه می‌برد. سـفری که گسـتره فوق‌العاده متنوعی از موضوعات را در بر می‌گیرد. موضوعاتی که عامه مردم و متخصصان را به یک اندازه مجذوب خود می‌کند.

محتوای کتاب

در این کتاب نویسـنده، برای آن که خودمـان و دیگران را عمیق‌تر درک کنیم، نشان می‌دهد:

- چگونه در اولین روزهای زندگی‌مان به ایده‌ها شکل می‌دهیم؟
- چگونه رویا می بینیم و تصور می‌کنیم؟
- چرا احساسات و هیجانات خاصی داریم؟
- مغزمـان چگونـه تغییـر می‌کند و ما همـراه با آن چگونـه تغییر می‌کنیم؟
- چگونه تصورمان در مورد خوب و منصف بودن خیلی زودتر از آنچه فکر می‌کنیم رشد می‌کند؟

زندگی پنهان ذهن از حوزه‌های فیزیک، ریاضیات، فلسـفه، پزشکی، زیست‌شناسـی، روانشناسی، مردم‌شناسـی، زبان‌شناسی و همچنین آشـپزی، شعبده بازی، شطرنج، موسیقی، ادبیات و هنر بهره می‌گیرد تـا نشـان دهد که علوم اعصـاب چگونه در زندگی بـه خدمت ما در می‌آید و عیان می‌کند که چگونه بی‌کرانگی نورون‌های درون مغزمان نحوه ادراک و احساس و استدلال و ارتباط ما را می‌سازند.

کتاب دارای فهرسـت مطالب، مقدمه، شش بخش مطلب، سخن آخر، ضمیمه، سـپاس‌گزاری و کتابنامه اسـت. عناوین بخش‌های کتاب به شرح زیر است:

بخش ۱: منشا تفکر.
بخش ۲: مرزهای نامشخص هویت.
بخش ۳: ماشینی که واقعیت را می‌سازد.

۱۳- استاد روان شناسی تجربی در کولژ دو فرانس
۱۴- دانشمند برجسته علوم اعصاب

بخش ۴: سفرهای آگاهی (یا به اشتباه انداختن آگاهی).
بخش ۵: مغز دائما در حال دگرگونی است.
بخش ۶: مغزهای تربیت شده.

عنوان کتاب: یادگیری ژرف.
نویسندگان: یان گودفلو، یوشوآ بنجیو و آرون کورویل.
مترجمان: سجاد ملکی و مائده حاجی آقا محسنی.
ناشر: نشر آتی نگر.
زمان نشر: ۱۳۹۷.
تعداد صفحات: ۵۰۴ برگ.
شمارگان: ۵۰۰نسخه.
شابک: ۹۷۸-۶۲۲-۶۱۰۲-۰۰-۱.
قیمت: ۵۵۰۰۰ تومان.

مقدمه

در مقدمه کتاب آمده است: موضوع این کتاب یافتن راه حلی برای مسائل شهودی‌تر است. این حل عبارت است از این که به کامپیوترها اجازه دهیم از تجربه‌ها بیاموزند و جهان را در قالب سلسله مراتبی از مفاهیمی درک کنند که هر مفهوم در قالب ارتباط خود با مفاهیم ساده‌تر تعریف می‌شود. این رهیافت از طریق گردآوری دانش حاصل از تجربه، نیاز به حضور کاربران انسانی، به منظور توصیف رسمی تمام دانش مورد نیاز کامپیوتر را بر طرف می‌کند. سلسله مراتب مفاهیم به کامپیوتر اجازه می‌دهد تا مفاهیم پیچیده را از طریق ساخت آن‌ها با استفاده از مفاهیم ساده‌تر، فرا بگیرد. اگر گرافی از نحوهٔ ساخت هر یک از این مفاهیم در راس یکدیگر رسم کنیم، یک گراف ژرف حاصل می‌شود که دارای لایه های متعدد است. به همین دلیل این روش را در هوش مصنوعی، یادگیری ژرف می نامیم.

محتوای کتاب

در مقدمه مفصل کتاب راهنمای خوبی برای مطالعه آن نوشته شده است. روندهای تاریخی یادگیری ژرف، نام‌های متعدد و سرنوشت متغیر شبکه‌های عصبی، اندازه رو به رشد مجموعه داده‌ها، تعدد مدل‌ها، دقت، پیچیدگی فزاینده و تاثیر بر جهان واقعی، مطالب مهمی است که در این مقدمه تشریح شده‌اند.
کتاب دارای فهرست مطالب، وبگاه، نمادگذاری، یک فصل مقدمه، دو بخش و یازده فصل مطلب است. عناوین بخش‌ها و فصول کتاب به شرح زیر است:

بخش اوّل: مبانی یادگیری ماشین و ریاضی کاربردی.
فصل ۲: جبر خطی.
فصل ۳: نظریه احتمال و اطلاعات.
فصل ۴: محاسبات عددی.
فصل ۵: اصول یادگیری ماشین.
بخش دوّم: شبکه‌های عمیق: شیوه‌های نوین.
فصل ۶: شبکه‌های پیش‌خور ژرف.
فصل ۷: منظم‌سازی برای یادگیری ژرف.
فصل ۸: بهینه‌سازی برای آموزش مدل‌های ژرف.
فصل ۹: شبکه‌های کانولوشنی.
فصل ۱۰: مدل‌سازی دنباله: شبکه‌های بازگشتی و تراجعی.
فصل ۱۱: روش شناسی کاربردی.
فصل ۱۲: کاربردها.

عنوان کتاب: اصول و مبانی وب معنائی.
تالیف و گردآوری : مرتضی نوروزی و محسن طاهریان.
ناشر: فرس.
زمان نشر: ۱۳۹۱.
تعداد صفحات: ۲۳۴ برگ.
شمارگان: ۱۰۰۰نسخه.
شابک: ۹۷۸-۹۶۴-۸۲۰۷-۱۸-۷.
قیمت: ندارد

مقدمه

مترجمان کتاب در پیش گفتار آن نوشته‌اند: هدف وب معنایی، پررنگ کردن نقش عامل‌های نرم‌افزاری یا به‌طور کلی ماشین‌ها در وب و تقویت قابلیت‌های آن‌ها در جهت کمک به انسان برای انجام راحت‌تر و سریع‌تر امور خود در وب می‌باشد. تقویت عامل‌های نرم‌افزاری مستلزم درک نسبی آن‌ها از معنای اطلاعات پراکنده در وب است ... برای گذار از وب کنونی به وب معنایی باید اطلاعات موجود در صفحات وب به گونه‌ای باز توصیف شوند که برای عامل‌های نرم‌افزاری هم قابل فهم باشند ... در کتابی که پیش روی شماست، تلاش شده با زبانی ساده اهم مفاهیم فناوری وب معنایی مشتمل بر زبان‌های موجود و ابزار مرسوم، تشریح گردد.

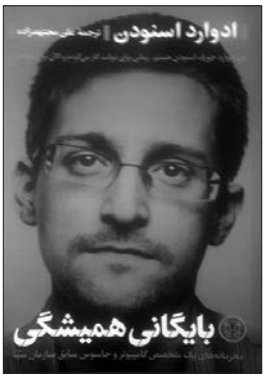
محتوای کتاب

هستی‌شناسی[15]ها در حقیقت شالودهٔ وب معنایی هستند. یک هستی‌شناسی با مشخص کردن مفاهیم و موجودات یک دامنه و توصیف روابط بین آن‌ها به‌صورت رسمی و قابل فهم توسط ماشین و با به خدمت گرفتن مجموعه‌ای از قواعد در حقیقت دانش موجود در آن دامنه را به‌صورت رسمی بیان می‌کند.

15- Ontology

کتاب دارای فهرســت، پیش گفتار و هفت فصل بدون عنوان مطلب و مراجع است. عناوین مطالب موجود در فصول کتاب به شرح زیر است:

فصل ۱: اصول وب، XML و وب معنائی.
فصل ۲: هستی شناسی و هستی شناسی در وب.
فصل ۳: RDF وگزاره‌ها و واژگان آن.
فصل ۴: RDF و RDF-S و زبان‌های هستی‌شناسی، OWL و OWL ۲.
فصل ۵: P3، Protégé-OWL و P4.
فصل ۶: SWRL، اجزا و ابزار و SQWRL.
فصل ۷: API.



عنوان کتاب: بایگانی همیشگی.
نویسنده: ادوارد اسنودن.
مترجم: علی مجتهد زاده.
ناشر: بنگاه ترجمه و نشر کتاب پارسه.
زمان نشر: ۱۳۹۸.
تعداد صفحات: ۳۶۰ برگ.
شمارگان: ۱۱۰۰ نسخه.
شابک: ۹۷۸-۶۰۰-۲۴۳۵-۵۲-۸.
قیمت: ۵۷۰۰۰ تومان.

مقدمه

نیویورکر درباره این کتاب نوشــته است: داســتان اینترنت، معشوق و کعبه آمال پســری که همه آزادی‌ها را در آن می‌دیده و در بزرگســالی ناگاه دیده که این آزادی در دستان دولتمردان به یغما می‌رود. واشنگتن پســت نوشــته اســت: کتابی دقیق که با زبانی کوبنده و محکم نوشته شــده و جزئیات مهمی از زندگی اســنودن را پیش چشم ما می‌گذارد. اکونومیست نوشته است: روایتی دقیق از جنایتی سازمان یافته به دست نهادهای اطلاعاتی آمریکا که خواندنش دل آدمی را به درد می‌آورد.

محتوای کتاب

بر پیشــانی جلد کتاب نوشــته شده اســت: من ادوارد جوزف اسنودن هســتم. زمانی برای دولت کار می‌کــردم و الان برای مردم. در ذیل نام کتاب بر جلد آن نوشته شده است: محرمانه‌های یک متخصص کامپیوتر و جاسوس سابق سازمان سیا. در زندگی‌نبشت نویسنده کتاب در کتاب آمده اســت: ادوارد بچه‌ای نه چندان معمولی، از خانواده ای نظامی بود. او ابتدا به ارتش رفت و از خدمت معاف شــد. سپس خود را به سازمان سیا رساند و بعد از مدتی به واسطه آنچه از کامپیوتر و اینترنت آموخته بــود به جایی برســد که امروز او را یکــی از نامدارترین هکرهای تاریخ می‌دانند. افشــاگری‌های ادوارد اسنودن از عملیات عظیم «جاسوسی و مراقبت در سطح جهانی» باعث شد تا به یکی از مهره‌های تحت تعقیب تمام نهادهای اطلاعاتی آمریکا تبدیل شود. بنا به مدارک اسنودن، این برنامه‌ها شــامل جاسوســی از مردم عادی و شــخصیت‌ها در مکالمات تلفنی، ایمیل و موتور جستجوی اینترنت در تمام کشورها بوده است. او اکنون در مکانی نامعلوم در روسیه زندگی می‌کند.

اســنودن در دیباچــه کتاب بــرای خوانندگانش در مور اســتحاله کار و دیدگاهش می‌نویسد: کاری که زمانی جمع آوری و انتقال اطلاعات بود، ابتدا چهره عوض کرد و به کاری بدل شد که هدفش ذخیره‌سازی دائمی و ابدی اطلاعات بود. بعدتر هم این شــد کــه چگونه بتوانیم اطلاعات را جوری ذخیره کنیم که از سراسر جهان هم بشود به آن دسترسی داشت و هم بتوان در آن به جستجوی داده‌های دلخواه پرداخت...تا آن زمان همه توان و دغدغه‌ام را پای این تفکر گذاشته بودم که انگار ما باید بدانیم و از همه چیز ســر در بیاوریم و اصلا درکی نداشتم که این کارها راه به کجا خواهد برد و تخصص من در خدمت چیست ... نشسته بودم توی اتاقی .... و تقریبا اگر هر مرد، زن یا بچه‌ای، در هر کجای جهان پشت کامپیوتری می‌نشست یا با تلفن شماره‌ای را می‌گرفت، می‌توانستم ردیابی‌اش کنم. آن ۳۲۰ میلیون نفر آمریکائی هموطنم هم در شــمار همین افراد بودند و ما با این کارمان نه تنها اصول اولیه قانون اساســی آمریکا که عرف هر جامعه آزادی را زیر پا می‌گذاشــتیم. اگر شما این کتاب را می‌خوانید به همین خاطر اســت که من به‌عنوان یک آدم دارای آن موقعیت، سرانجام دست به کاری زدم که بسیار خطرناک بود. من حقیقت را به صدای بلند گفتم. من همه اسناد داخلی و مدارکی را که نشان می‌داد جامعه اطلاعاتی امریکا قانون‌شکنی کرده است جمع‌آوری کردم و به‌دست روزنامه نگارها رســاندم که آن را به گوش مردم جهان برســانند ... برای نسل من، همه معنای ارتباط، تنها و تنها در اینترنت خلاصه می‌شد. پس نزنید! می‌دانم که الان اینترنت چه پدیده مسموم و مشئومی‌شده، اما بگذارید این نکته را یادتان بیاورم، آن زمان که من تازه با اینترنت آشــنا شــدم، این پدیده به کل چیز دیگری بود. اینترنت هم دوســت ما بود و هم یکی از والدین مان...حالا می‌فهمید که وقتی می‌گویم دیگر از اینترنت این زمانه سر در نمی‌آورم، منظورم چیســت ... این دگرگونی کاملا آگاهانه رخ داده ... آن هجوم بی‌سابقه به اینترنت برای تبدیل بازارها به پدیده‌های الکترونیک(ی) خیلی زود حبابی را شــکل داد که به ســرعت و در هزاره جدید ترکید ... شــرکت‌ها خیلی زود فهمیدند که مردم در اینترنت، بیشتر از پول خرج کردن به اشــتراک گذاری (اطلاعاتشان) فکر می‌کنند و بهتر است روی همین میل مردم به ارتباطات انســانی (از طریق اینترنت) سرمایه‌گذاری کنند. وقتی آدم‌ها دوســت دارند فقط روی اینترنت با هم حرف بزنند و خبر از هم بگیرند و به دوســتان، خانواده و دیگران و حتی غریبه‌ها خبر بدهند که الان کجا هستند و چه می‌کنند، دیگر کار شرکت‌ها تنها این شد که چگونه خودشان را در مسیر این رابطه انسانی قرار دهند و از آن رهگــذر پولی به جیب بزنند. پایان کار اینترنتی که من می‌شــناختم را همین رقم زد، نظام سرمایه‌داری نظارت...تازه فهمیده بودم که این نظارت عمومی و تبعات منفی آن چیست.

کتاب بایگانی همیشگی غیر از وجوه روشنگرانه کم‌نظیر، داستانی خواندنی از وجدانی بیدار شده می‌نماید و شامل شرح حال مختصر نویسنده و سه بخش مطلب بی‌عنوان است که خواندن آن توصیه کردنی است.

در مورد ریسک و بختانگی

علیرضا خلیلیان، دانشجوی دکتری نرم‌افزار، دانشگاه اصفهان

پست الکترونیکی: khalilian@eng.ui.ac.ir

ORCID: 0000-0002-4079-703X

یادداشت: در اسفند ماه ۹۸ توفیق یافتم و کتاب «قوی سیاه، اندیشه‌ورزی پیرامون ریسک» نوشته نسیم نیکلاس طالب و ترجمه دکتر محمد ابراهیم محجوب را مطالعه کـردم. پس از اتمام کتاب حدود پنج صفحه از نکات املایی، ترجمه‌ای و موارد جا افتاده را برای مترجم ارسال کردم. ایشان در همان موقع مشغول آماده‌سازی نسخهٔ صوتی و ویرایش ششم کتاب بودند و از دیدن این موارد بسیار خوشحال شدند. آشنایی ما ادامه پیدا کرد تا در بهار ۹۹ به پیشنهاد ناشر گفت‌وگوی زنده‌ای در اینستاگرام با ایشان و ناشر برگزار کردیم. مطالب این مقاله بخشـی از آموزه‌های من در مورد ریسک است که با شما در میان می‌گذارم.

بنابر پژوهش‌های بهاءالدین خرمشاهی در کتاب «فرهنگ-دانشنامه کارا» واژه انگلیسی «ریسک» به واژه «روتیک» در زبان پهلوی و «رزق» در عربی برمی‌گردد. و واژه رزق و روزی اغلب در فارسـی باهم می‌آیند. ما همگی معتقدیم که رزق و روزی مخصوص خداوند است و باوجود این‌که ما تلاش می‌کنیم ممکن اسـت روزی مطلوب را به‌دسـت بیاوریم یا نه. نظامی در کتاب «خسرو و شیرین» از مجموعه «خمسه» خود می‌گوید:

چو روزی بخش ما روزی چنین کرد / گهی روزی دوا باشد گهی درد

یا حافظ در دیوان خود می‌گوید:

بشنو این نکته که خود را ز غم آزاده کنی / خون خوری گر طلب روزی ننهاده کنی

دنیایـی که در آن زندگی می‌کنیم کاملاً غیرقطعی اسـت و پر اسـت از رویدادهای «بختی». ما ممکن اسـت در هر کاری حداکثر تلاش خود را انجام دهیم اما از سـایر عوامل تاثیرگذار بی‌خبریم و این‌طور می‌شود که گاهی روزی منفی به ما می‌رسـد؛ یعنی ممکن است ضرر کنیم یا درد و مصیبتی به ما برسد. ریسک هم تقریباً با چنین معناهایی تفسیر می‌شود. پدیده‌هایی هسـتند که از ترکیب دو وجه رخ می‌دهند: یکی «اراده ما» و دیگری «قضا، سرنوشت و بخت» و مسئله اینجاست که ما از پیش سهم و ترکیب این‌دو را نمی‌دانیم.

ریسـک دو بُعد دارد: یکی «احتمال» وقوع پدیده و دیگری «پیامد»، اگر پدیده رخ دهد. و ریسـک دو دسته مثبت و منفی دارد. به ریسک مثبت می‌توان گفت «امیدِ سـود» و به ریسک منفی هم «بیمِ زیان» که امید و بیم احتمالند و سود و زیان هم پیامد هستند. یک مدیر ریسک نه تنها باید احتمال رخداد را درنظر بگیرد، بلکه بیشتر باید پیامد موضوع را مورد نظر قرار دهد. سعدی در «گلستان» خود می‌گوید:

غواص گر اندیشه کند کام نهنگ / هرگز نکند دُرّ گرانمایه به چنگ

فردی ممکن اسـت سـاعت ۱۲ ظهر از خیابان شلوغی عبور کند. در این حال احتمال تصادف او زیاد اسـت اما به احتمال زیاد خسـارت زیادی از تصادف نمی‌بیند. اما همان فرد اگر ساعت ۱۲ شب از همان خیابان عبور کند، به‌خاطر خلوتی احتمال تصادف خیلی کم است، اما در صورت تصادف ممکن است پیامد سنگینی مثل خسارت جانی در پی داشته باشد.

مما در متنی که آمد از واژه «بختی» اسـتفاده شد. این واژه ترجمه «ran-dom» اسـت که در متون مختلف از جمله رشته‌های مختلف کامپیوتر رایج است. این واژه را اغلب «تصادفی» ترجمه می‌کنند. اما بنابر بحث دکتر محجوب در مقدمه کتاب قوی سیاه، منظور از تصادفی «بی‌قصدی» است درحالی‌که منظور ما از رَندوم «بی‌الگویی» است. در جملهٔ «He opened Hafez at random» منظور ما این نیست که دست فرد بی‌قصد خورده و کتاب ناگهان باز شـده است. فرد عمداً سراغ کتاب رفته و از روی قصد کتـاب را باز کرده اما در باز کردن کتاب الگویی نداشـته و صفحه‌ای که باز شـده قابل پیش‌بینی نبوده است. دکتر محجوب ایده این معادل را از لغت‌نامه پنج جلدی «فرهنگ-دانشنامه کارا» گرفته است که به سرپرستی بهاءالدین خرمشـاهی نوشـته شده و توسط نشر شـباهنگ در سال ۹۴ منتشـر شده است. یک مزیت این فرهنگ اینسـت که با واژگان مصوب فرهنگستان سنجیده شده اسـت. در این فرهنگ برای واژه «random-ly» معادل «بختانه» پیشنهاد شده است. به این‌ترتیب دکتر محجوب نیز وفق دستور زبان فارسـی واژه «بختانگی» را به‌عنوان اسم مصدر در برابر «randomness» قرار داده‌اند.

مراجع

۱- نسیم نیکلاس طالب، قوی سیاه اندیشه‌ورزی پیرامون ریسک، انتشارات آریانا قلم، چاپ پنجم، ۱۳۹۸.

۲- بهاءالدین خرمشاهی، فرهنگ-دانشنامه کارا، نشر شباهنگ، ۱۳۹۴.

سرگرمی

- بعضی آدما مثل به‌روزرسانی نرم‌افزارند. وقتی می‌بینمشان فکر می‌کنم «حالا نه»

* * *

- یک روز سرد زمستانی، خانمی به همسرش پیامک فرستاد که «پنجره‌ها انگار یخ زده‌اند، باز نمی‌شوند» همسرش جواب داد که «کمی آب ولرم رویشان بریز و به آرامی با چکش به لبه‌هایشان بزن.» پنج دقیقه بعد، خانم پیامک فرستاد «کامپیوترمون داغون شد.»

* * *

- هر کسی گفت معنی دیوانگی اینه که یک کار را بارها و بارها انجام بدین و انتظار نتایج متفاوتی داشته باشین، بدونید که هرگز مجبور نشده کامپیوترش را ریبوت کنه.

* * *

- در یک فروشگاه بازی‌های کامپیوتری، شنیدم خانمی به فروشنده گفت «من یک بازی می‌خوام که مورد علاقهٔ بچهٔ شش ساله‌ام باشه. منتها باید به قدر کافی ساده باشه که باباش هم بتونه بازی کنه.»

* * *

- بعد از این که یک کامپیوتر شخصی نو خریدم، با اشتیاق فراوان به خانه آمدم، جعبه‌اش را باز کردم و آن را به به برق زدم امّا انگار مرده بود. هیچ چراغی روشن نشد و هیچ اتفاقی نیفتاد. به فروشنده زنگ زدم و ماجرا را تعریف کردم.
- فروشنده: کامپیوتر را روشن کرده‌اید؟
- البته که روشن کرده‌ام.
- فروشنده: آیا پشت کامپیوتر را باز کرده‌اید تا ببینید هیچیک از تخته مدارها در هنگام حمل و نقل شل نشده باشد؟
- البته، این کار را هم کردم. همه سرجایشان محکم بودند.
- فروشنده: خوب، برای چی به من زنگ زده‌اید؟
- خوب شما این را به من فروخته‌اید و لابد ضمانت هم دارد.
- فروشنده: البته که دارد امّا شما با بازکردن پشت کامپیوتر، ضمانتش را بی‌اعتبار کردید!

* * *

- دو محصول عمده که از دانشگاه برکلی بیرون آمده است: LSD و UNIX. ما فکر نمی‌کنیم که اتفاقی بوده باشد.

* * *

سؤال: چه فرقی بین فروشندهٔ ماشین و فروشندهٔ کامپیوتر است؟
جواب: فروشندهٔ ماشین احتمالاً رانندگی بلد است.

* * *

مشتری: سیستم عامل کامپیوتر من ویندوز ۹۸ است.
پشتیبان فنّی: خوب، چه مشکلی پیش آمده؟
مشتری: کامپیوترم کار نمی‌کند.
پشتیبان فنّی: بله، این را که قبلاً گفتید.

* * *

کامپیوترها هوشمند نیستند. آن‌ها فقط فکر می‌کنند که چنین هستند.

* * *

- دوست داری یک کامپیوتر دست دوم بخری؟
- نه، فکر نکنم. من فقط می‌تونم با یک دست تایپ کنم.

لیست اعضای حقوقی

انجمن انفورماتیک ایران

اعضای حقوقی فعال در حوزه راه‌حل‌های برنامه‌ریزی منابع سازمان و نرم‌افزارهای پیشرفته سازمانی

- آفرینش رایانه کیهان
- آریانا پرداز آینده
- ایریسا (بین‌المللی مهندسی سیستم‌ها و اتوماسیون)
- بهکو (بهینه کوشان سپهر)
- برگ سیستم پویا
- پارس رویال نفیس
- پارس اوک کیش
- پارس تصمیم
- پردازش موازی سامان
- پردازش اطلاعات ریسمان
- پویندگان تجارت دهکده جهانی
- توسعه یکپارچه ایلیا
- تدوین فرآیند
- تحقیق و توسعه ارتباط
- تیم یار کیش
- چارگون
- درگاه ارتباطات جدید
- راهکارهای برتر یکپارچه ساپارد اروین
- رایاوران توسعه
- راهبر نیروی خراسان (رانیر)
- مهندسی رای دانا آفرین
- سامانه پرداز اریس
- پایه‌ریزان راه‌کارهای فراگیر
- سامه آرا پردازشگر
- سبز داده افزار
- سیستم‌های اطلاعات مدیریت شرق رایا
- سیما رایان روز
- سند پرداز
- شماران سیستم
- شرکت باران آبی بلورین
- شرکت فنی و مهندسی و خدماتی پیام صنعت صدرا
- گروه نرم‌افزاری پیوست
- گلرنگ سیستم
- فناوری نوین رایا شریف
- فرابوم کسب و کاری نو آوری باز
- فناوری اطلاعات و ارتباطات پاسارگاد آریان (فناپ)
- داده‌ورزی فرادیس البرز
- نوید ایرانیان (گسترش فضای مجازی)
- نماتک ایرانیان
- مانیر (مشاورین انفورماتیک نیرو)
- مهندسی بهینه ایران
- مدیریت سیستم های دیجیتال
- مهندسی نرم‌افزاری رایورز
- مهندسی نرم افزار فرارای (سهامی خاص)
- مبنا داده ارتباط شبکه
- نماد ایران
- داده پردازی نیلرام مانا

لیست اعضای حقوقی

انجمن انفورماتیک ایران

گروه مشاورین ورانگر نوین

کومشیان پارت پیشرفته

گام الکترونیک

همکاران سیستم

هورماه رابین خاور

مشاوران یام آذر

اعضای حقوقی فعال در حوزه نرم‌افزارهای کاربردی

آریا ایمن تدبیر

آناد صنعت سپهر

آریاز بهگران کسب و کار

آریو برزن نوین

آمایشگران تجارت کامیاب

ایده زرین پرهام

اپلیکشن پوستر

اطلاع‌رسانی پیوند داده‌ها

ایران رایانه

اصحاب رسانه پویا

ایده‌پرداز تجارت مهر آفاق

آریانا پرداز آینده (آرپا)

انتقال دانش صنعت انرژی برق

پندار کوشک ایمن

پژند الکترونیک

پردازش اطلاعات و ارتباطات هاماوران آسیا

توسعه هوش موازی

توسعه ارتباطات رایانه‌ای آبانگان

توسعه فناوری اطلاعات جهان افزارنوین

تدبیرگران نوآوری رایسان

تیم تعمیرات و نگهداری خطوط لوله خاورمیانه

خدمات مهندسی فن آوری های طیف گستر اطلس طاها

خبره حسابان ره آورد

چشم انداز تجارت به دان

داده پردازان احداث

داده کاوان پیشرو ایده ورانگر

رایان پرتو نگار

سنجه حساب

سروش رایانه ایرانیان

سامانه های یکپارچه سیمرغ تجارت

شایگان سیستم

شرکت داده پرداز ماکان سیستم دانشمند

صنایع فن آوری طراحان بهینه

مهندسی تکرو سیستم

مهندسی نرم افزار فرا پیام

مهندسین مشاور نقش بوستان گستر

مجتمع داده‌ها و سیستم‌ها (MDS)

موسسه حقوقی و مطالعات اقتصادی آرمان ایرانیان

فاوا وب بیست و چهار

فناوری ارتباط امن خاورمیانه

فن آوران مشاور همراه آسایش

لیست اعضای حقوقی

انجمن انفورماتیک ایران

فناوری نوین زنجیره بلوکی سگال

همراهان سیستم گوهر

یوتاب ارتباطات آرینا

نرم‌افزاری امن پرداز

شرکت نواندیشان مدیا نام

شرکت ویرا سگال کارو

رهیاب ریان فردا

مدار گسترش فناوری اطلاعات

کیان سرویس صدرا

گروه فنـاوری اطلاعـات و ارتباطات هیواتک

گروه شرکت های مهندسی نرم افزار فراپیام

گروه فناوری اطلاعات آتیه ویستانگر

گستره چتر نیلی

عصر امار و فناوری اطلاعات

اعضای حقوقی فعال در حوزه بانکی و بانکداری الکترونیکی

الماس هوشمند ایرانیان

آسمان صبح فردا

ارتباطات هدی ارقام

الکترونیک تراکنش ویرا

بهسازان ملت

بانک اقتصاد نوین

بانک آینده

به‌پرداخت ملت

پدیسار انفورماتیک ایران

پرداز گستر تدبیر

پردازشگران سامان

پرداخت اکترونیک سداد

پویا

پردازش اطلاعات مالی پارت

پایا انرژی باتاب

توسعه سامانه‌های نرم افزاری نگین

توسعه فن آوران لوتوس شبکه

توسعه فناوری رفاه پردیس

توسعه خدمات الکترونیکی آدونیس

ثامن ارتباط عصر

تامین کالای پتروسینا

تجارت الکترونیک پارسیان کیش

تلکام سافت

شرکت کسب و کارهای نوپای خاورزمین

شرکت راهکارهای هوشمند و یکپارچه آسا

ماتریس تحلیلگران سیستم‌های پیچیده

خدمات انفورماتیک

توسعه تجارت الکترونیک نگین توسن

خدمات ماشین‌های اداری امیم رایانه

سامان امنیت پرداز کیش

سفیر آبی آرام

شرکت مهندسی آتی سازاب ایرانیان

لیست اعضای حقوقی

انجمن انفورماتیک ایران

شرکت توسعه ارتباطات الکترونیک تجارت ایرانیان

شرکت سامان ایمن پرداز شرق پاژ

شرکت صنایع الکترونیک فاران

شرکت توسعه فن‌افزار توسن

داده‌پردازی ایران

رایانه خدمات امید

شرکت مشاوره رتبه بندی اعتباری ایران

سامانه تبادل الکترونیک دفاتر پیشخوان دولت

سامانه واریزی

مشاورین بهبود روش‌ها و سامانه‌های مبنا

فاوا هزاره کیش

فن‌آوران اطلاعات آسام

فناوری اطلاعات ناواکو

فرانگر صنعت کارت اریا

گرایش تازه کیش

گسترش فناوری‌های نوین

توسعه فناوری اطلاعات خوارزمی

صنایع پرسو الکترونیک

اعضای حقوقی فعال در حوزه اینترنت و پورتال‌ها

آسیانت چهارمحال

ارتباطات مبین نت

افرا فناوری ایکاد

بهسو نوران نارین

افرانت

فرا ارتباط کویر کاشان

پارس لین

تندیس تلاش و تفکر

توسعه فناوری ریز فن پردازش پرشین

داده پردازی پویای شریف

داده پردازان اسپیناس وب

رایان هوشمند نویان

روند تازه

دانش افزار نارون شریف

فناوری اطلاعات و ارتباطات پارس پردازش سدید

فن‌آوری اطلاعات پارسیان میزبان

شرکت فن آوری اطلاعات لونا پارس

فرابرد داده‌های ایرانیان

فناوری رادین پاسارگاد

شرکت فن‌آوری اطلاعات لونا پارس

کیانا پارسیان کیش

کلیدگستر آینده (نت بینا)

گروه شرکت‌های فن‌آوا

مؤسسه گسترش اطلاعات و ارتباطات و فرهنگی ندا رایانه

هاست ایران

شرکت هزار یک فرصت

اعضای حقوقی فعال در حوزه شبکه و سخت‌افزار

آوید رایانه هیراد

لیست اعضای حقوقی

انجمن انفورماتیک ایران

آلبالو رایانه سخت افزار

آرین وب ایرانیان

آرسسس پارت پرداز قرن

ایمن تصویر مهرگان

ایمن سازان تارنمای ایرانیان

امن پرداز ان سورنا

ارم تک مبین

امواج گستر نوین

بانی رایان پرداز نو

توسعه فناوری برنا پارسه

توسعه فناوری تجارت حکمت

توسعه و تجهیز فدک رایان

پارس فایبرنت

پیشتازان اندیشه پویا

سرو حامی پارس

سیستم افزار خاورمیانه

شرکت مهندسی پیما عمران نیرو

شرکت شبکه بانان پاژ

شرکت تجارت سرور ماندگار

شرکت آوای همراه هوشمند هزاردستان(کافه بازار)

شرکت مهندسی سیستم‌های اطلاعاتی پیشرو

شبکه گستر فن آوا

توسعه سرمایه گذاری گروه آروند

برد پرداز رایانه

بهاور فناوری ویرا

پارسیان فیبر ارتباط

پرتو بیتا جاوید

پیشرو توسعه نوآوران آرتا

ترویج صنعت سومی پارسیان

تحلیلگران شبکه گستر پارسه

تحلیلگران اطلاعات نگاره

تحلیلگران ارتباط ایرانیان

توسعه داده‌پردازی بنیس

تامین و توسعه فناوری کوثر

توسعه فن آوری ارتباطات و اطلاعات راهکار مفید پرداز

توسعه صنایع زیر ساخت سگال فرتاک

دانشگاه آزاد علوم تحقیقات خوزستان

شرکت رایانه همراه کیان

رایان مهر الکتریک

رابین نوآوری برساد

رادمان داده‌پردازی فرنام

رهنمون فناوری اطلاعات

خدمات کامپیوتری خانه سیستم

خدمات رایانه ای بهینه پرداز پویا

رایان ارتباط گستر تاو

داده پردازان فن‌آوری اطلاعات و ارتباطات جم

سرو رایانه

سیمرغ سامانه تهران

لیست اعضای حقوقی

انجمن انفورماتیک ایران

شبکه گستر نسل جدید

فرا ارتباط گستر پویا

فناوران اهل قلم نوین

فناوری اطلاعات سهلان

فرصت کیش

مهندسی ارتباطات دوربرد فارس

مفتاح رایانه افزار

مهندسی رادین راهبرد رایانه

شایان توسعه البرز

شبکه پایدار فناوری اطلاعات

شرکت ویرا اندیش خاورمیانه

شبکه هوشمند پدیده آپادانا

صباکاربردلتا

صنایع پرسو الکترونیک

شرکت مهندسی گسترش ارتباطات نو خاورمیانه

شرکت توسعه ارتباطات پویا اندیش

فن‌آوری اطلاعات و ارتباطات آرمان تندیس ایرانیان (فن آرا)

کاسپین آبی آریانا

کارنما رایانه

کیسان صنعت ایرانیان

کیسون

گروه مهندسین فرایند

گروه بازرگانی آریانا پارس راژمان

لایف سرویس پارسه

مهندسی رایان توان افزار

ماهان شبکه ایرانیان

شرکت ماکان پرتو پردازش خاورمیانه

مهندسی شبکه گستر

مهندسی کارن پارت شرق

مهندسی افق داده ایرانیان

مهندسین مشاور ارتباط گستران شرق

نوین ارتباط نوآوا

نوآوران سامانه سهند ایماژ

شرکت

اندیشه‌پرداز دوران

انتقال داده پرشین

ویژن پلاس اروپا

نگرش تحلیل سیستم‌ها

نویان ابر آوران

نوآوران اندیش رایانه غرب

نوین داده پرداز روناش

یاشار طرح آذربایجان

اعضای حقوقی فعال در حوزه مدیریت پروژه

پروژه کاران کوروش پرشیاً

فناوران اطلاعات بهاران

اندیشه وران

سامانه ورز هزاره

کامپیوتری خانه سیستم

لیست اعضای حقوقی

انجمن انفورماتیک ایران

مدیریت پروژه نیروگاه‌های سولار

ماهان شبکه ایرانیان

اعضای حقوقی مشتریان بهره‌بردار از راه‌حل‌های نرم‌افزارهای پیشرفته سازمانی و بهره‌بردار از فناوری اطلاعات

ایریسا

استاندارد تکنولوژی کایند

اتصال صنعت میانه

پارسین تجارت پایا کیش

پردیس خدمات هزاره کیش

توزیع برق آذربایجان

شرکت توسعه فناوری آریا رهجو

ترابری بین المللی پرس

تجارت الکترونیک تدبیر کیش

پردازش هوشمند البرز

خدمات مشاور خرد پیروز

زورق آرامش

راه آرمان مهر نیکان

شرکت فناوری اطلاعات سات بان

شرکت توسعه خدمات مراکز داده پیشرو

مهندسی و ساخت بویلر مپنا

گروه کارخانجات چینی مقصود

گسترش فناوری اطلاعات ستاره ویدا

مهندسی آریا تدبیر ایلیا

مهندسی شریف برودت

طبیعت‌زنده

فن‌آوران سپاکو رایانه

فن‌آوری اطلاعات ویژن

نوین پردازان آتیه عصر ویرا

اعضای حقوقی فعال در حوزهٔ آموزش و پژوهش

آکادمی یاسان

آماج فناوری اطلاعات وارتباطات ایرانیان

الماس رایان ایرانیان

پژوهشگاه ارتباطات و فناوری اطلاعات

پژوهشکده آفافق دانش خوارزمی

سماتک

فناوری اطلاعات بین‌الملل

مؤسسه عالی مدیریت دانش

کهکشان نور

شرکت علم یاران

گروه فنی مهندسی ایده سازان مبتکر قرن

گذرگاه امن آسیا

مهندسی اوژن تدبیر پارس

اعضای حقوقی فعال در حوزهٔ مشاوره

الهه کوچک نرم افزار

تیوا سیستم

موسسه حقوقی واقتصادی آرمان ایرانیان

طرح و توسعه الکترونیک افق

سرآمد فناوری اطلاعات

شرکت مشاور فن آوران و اطلاعات فهامه

شرکت شبکه گستر ساینا

مهندسی کاربرد سیستم سدید