مدیریت فناوری اطلاعات
دانشکدهٔ مدیریت دانشگاه تهران
دورهٔ ۷، شمارهٔ ۳
پاییز ۱۳۹۴
ص. ۵۳۰- ۵۱۱

طراحی سیستم خبرهٔ فازی برای مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها

شعبان الهی[۱]، مصطفی رشیدی[۲]، محمود صادقی[۳]

چکیده: مدیران عالی حریم خصوصی با نقش‌ها و مسئولیت‌های متنوع و متعددی مواجه‌اند. از این رو، به‌منظور آگاه‌کردن مدیر عالی حریم خصوصی از وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، در این مقاله نوعی سیستم خبرهٔ فازی با نام «سیستم خبرهٔ فازی مدیر عالی حریم خصوصی» طراحی شده است. به‌منظور تدوین مدل پژوهش و پایگاه دانش سیستم خبرهٔ یادشده، مفاهیم شایستگی مدیر عالی حریم خصوصی، نیت جرایم الکترونیکی، نوع تبادلات الکترونیکی بین دولت و کسب‌وکارها، اخلاق‌مداری حرفه‌ای طرفین تبادلات الکترونیکی و فناوری‌های محافظ حریم خصوصی شرکت، مؤلفه‌های وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها شناسایی شدند. به‌منظور اعتبارسنجی سیستم خبرهٔ فازی مدیر عالی حریم خصوصی، مقایسه‌ای از خروجی‌های سیستم پیشنهادشده با نظر خبرگان به عمل آمد. این سیستم، به تحلیل حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها و ارائهٔ توصیه‌های دقیق‌تر، کمک می‌کند.

واژه‌های کلیدی: تبادلات الکترونیکی دولت و کسب‌وکار، سیستم خبره، مدیر عالی حریم خصوصی، منطق فازی.

۱. دانشیار مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران
۲. کارشناس‌ارشد مدیریت فناوری اطلاعات، دانشکدهٔ مدیریت و اقتصاد، دانشگاه تربیت مدرس، تهران، ایران
۳. دانشیار حقوق خصوصی، دانشکدهٔ حقوق، دانشگاه تربیت مدرس، تهران، ایران

تاریخ دریافت مقاله: ۱۳۹۳/۱۲/۰۹
تاریخ پذیرش نهایی مقاله: ۱۳۹٤/۰٤/۱۳
نویسندهٔ مسئول مقاله: شعبان الهی
E-mail: Elahi@modares.ac.ir

مقدمه

در قلب فرهنگ اینترنت، نیرویی وجود دارد که می‌خواهد هرچیزی را دربارهٔ شما، کشف کند. اطلاعات شخصی افراد و اسرار تجاری شرکت‌ها، دارایی‌های با ارزشی هستند که دیگران را برای تجارت دربارهٔ آن اطلاعات و اسرار، وسوسه می‌کند. آندره گرو، یکی از مدیران اجرایی شرکت اینتل، نسبت به مسئلهٔ حریم خصوصی در اینترنت ابراز نگرانی می‌کند و می‌گوید: حریم خصوصی، یکی از بزرگ‌ترین مسائل در عصر الکترونیکی جدید است. اگر برخی از شرکت‌ها، به‌اندازهٔ کافی نسبت به مسئلهٔ حریم خصوصی ذی‌نفعان (مشتریان)، کارکنان، سهامداران، شرکای تجاری، تأمین‌کنندگان و سایر اشخاص حقیقی و حقوقی توجه نکنند، سهم بازارشان را از دست می‌دهند (بامبرگر و مولیگان، ۲۰۱۱؛ رزمیرسکی و سیسه، ۲۰۰۲؛ آوازو و دسوزا، ۲۰۰۴ و ردیک و روی، ۲۰۱۳). مدیران عالی حریم خصوصی کسب‌وکار با مسائلی از جمله ترکیب نقش‌های چون مسئول حریم خصوصی، مسئول رسیدگی به شکایت‌ها در دعاوی حقوقی بین شرکت و نهادهای دولتی، سرپرست اسناد و مدارک شرکت و نیز، چندبرابربودن خطر تبادلات آنلاین دولت با اشخاص حقیقی و حقوقی نسبت به مبادلات تجاری، مواجه‌اند. از سویی، سیستم‌های خبره، برنامه‌های هوشمند رایانه‌ای هستند که از دانش و رویه‌های استنتاج برای حل مسائلی استفاده می‌کنند که به اندازهٔ کافی دشوارند و به تخصص خاص انسانی، نیاز دارند. این سیستم‌ها می‌توانند کاربر را در حل مسئله راهنمایی کنند و دانشی را که از اسناد و متخصصان دریافت کرده‌اند را در اختیار کسانی قرار دهند که به آن دانش نیاز دارند. در واقع سیستم‌های خبره می‌توانند مانند مشاوری در کنار متخصصان انواع حوزه‌ها، به‌کار گرفته شوند (الهی، خدیور و حسن‌زاده، ۱۳۹۰؛ دن باتر، لیو و تان، ۲۰۱۲؛ شمسی، ۱۳۹۲؛ قدس الهی، ۱۳۸۹ و جالتا، بودوریک و ژانگ، ۲۰۰۶). در اینجا نیاز به نوعی سیستم خبره به‌منظور آگاه‌سازی مدیر عالی حریم خصوصی از وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، احساس می‌شود. سؤال‌های زیر به‌منظور شناخت بهتر مسئله مطرح شده‌اند:

۱. چگونه می‌توان شبکهٔ مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها را طراحی کرد؟
۲. چگونه می‌توان دانش و تخصص مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها را مدل‌سازی کرد؟
۳. چگونه سیستم خبره می‌تواند به مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها کمک کند؟

به‌منظور رعایت انسجام ساختار پژوهش، این مقاله بدین شرح نگاشته شده است؛ در ادامه، سیستم‌های خبره در نشریه‌های معتبر بررسی می‌شود، روش‌شناسی پژوهش بخش بعدی را شکل می‌دهد و پس از آن به چگونگی استخراج مدل مفهومی و سیستم خبرهٔ فازی پیشنهادشدهٔ این پژوهش با عنوان «سیستم خبرهٔ فازی مدیر عالی حریم خصوصی»[1] اشاره می‌شود، این مقاله با ارائهٔ یافته‌ها و نتایج به پایان می‌رسد.

پیشینهٔ نظری پژوهش

مقالهٔ وارن و براندیس در سال ۱۸۹۰ با عنوان «حق مصونیت حریم خصوصی»، اولین بحث جدی و صریحی بود که موضوع حریم خصوصی افراد را در چارچوب قوانین حقوقی مطرح کرد. در سال ۱۹۶۷ وِستین با انتشار کتاب *حریم خصوصی و آزادی*، ضمن تکمیل تعریف حوزهٔ حریم خصوصی، مبنای چهارگانه‌ای برای حریم خصوصی افراد تعیین کرد. وِستین، انقلاب و سیر تحول حریم خصوصی اطلاعات را با پیروی از انقلاب فناوری اطلاعات، طی چهار مرحلهٔ زیر شرح داد (جالتا، بودوریک و ژانگ، ۲۰۰۶؛ جنسن، پاتز و جنسن، ۲۰۰۵ و اصلانی، ۱۳۸۴: ۲۶- ۱۸ و ۶۶-۵۹):

۱. آغاز و مبنای حریم خصوصی (۱۹۶۰- ۱۹۴۵): اعتماد زیاد به بخش کسب‌وکار و دولت و راحتی جمع‌آوری اطلاعات همراه با توسعه‌های فناوری اطلاعات محدود؛
۲. اولین دورهٔ توسعهٔ حریم خصوصی معاصر (۱۹۷۹-۱۹۶۱): مطرح‌شدن ریسک حریم خصوصی اطلاعات با عنوان مسئلهٔ قانونی، سیاسی و اجتماعی صریح، تشخیص اولیه از جناح‌های تاریک فناوری‌های جدید و تدوین چارچوبی برای راهکارهای اطلاعاتی منصفانه و تنظیم قانون حریم خصوصی در سال ۱۹۷۴؛
۳. دومین دورهٔ توسعهٔ حریم خصوصی معاصر (۱۹۸۹-۱۹۸۰): طراحی سیستم‌های رایانه‌ای، قابلیت‌های پایگاه‌های داده‌ای و شبکه‌کردن فناوری‌های جدید درون راهکارهای اطلاعاتی منصفانه؛
۴. سومین دورهٔ توسعهٔ حریم خصوصی معاصر (۲۰۰۳-۱۹۹۰): تغییر چشم‌انداز مبادلهٔ اطلاعات توسط اینترنت و وب ۲/۰ و حمله‌های تروریستی ۱۱ سپتامبر.

اروین آلتمن در سال ۱۹۷۵ با هدف توصیف این موضوع که چرا مردم گاهی ترجیح می‌دهند در تنهایی بمانند و گاهی مایل‌اند در تعاملات اجتماعی درگیر شوند، نظریهٔ مقررات حریم

1. Chief Privacy Officer Fuzzy Expert System (CPOFEX)

خصوصی[1] را توسعه داد و بیان کرد، حریم خصوصی ایستا و ثابت نیست، بلکه کنترل گزینشی از دسترسی به اطلاعات شخصی فرد است. در واقع مبانی نظری دربارهٔ حریم خصوصی تبادلات دولت و کسب‌وکار، هنوز در دوران کودکی قرار دارد و اغلب تبادلات دولت و کسب‌وکارها در اتحادیهٔ اروپا تا سال ۲۰۰۷، غیرالکترونیکی و مبتنی بر کاغذ بوده است (بلداد، جانگ و استیهودر، ۲۰۱۰؛ بلنگر و هیلر، ۲۰۰۶ و الهی و حسن‌زاده، ۲۰۰۹)؛ به‌طوری‌که تاکنون سیستمی به‌منظور بررسی حریم خصوصی تبادلات دولت و کسب‌وکار طراحی نشده است.

پیشینهٔ تجربی

با توجه به پژوهش‌های پیشین در حوزهٔ سیستم‌های خبره و حریم خصوصی و امنیت شرکت‌ها، در این بخش به بررسی انتقادی آنها پرداخته شده است. لانگلی و ریگبای (۱۹۹۲) با استفاده از برنامهٔ پرولوگ و مدل مبتنی بر قاعده، به طراحی سیستم خبره‌ای برای به‌کارگیری طرح‌های مدیریت کلید در مدل‌های امن سیستم‌های رمزنگاری در شبکه‌ها اقدام کردند. در سال ۱۹۹۵ کایلای و جارات، به‌منظور مدیریت و تحلیل ریسک امنیت رایانه‌ای، نوعی سیستم خبرهٔ کیفی برای سازمان‌های تجاری کوچک و متوسط توسعه دادند. کارات، کارات، برودیه و فنگ در سال ۲۰۰۵، به‌منظور تسهیل تألیف، قبول پایش، پیاده‌سازی و به‌کارگیری خط‌مشی حریم خصوصی و شناسایی احتیاجات حریم خصوصی سازمانی، سیستمی طراحی کردند که به روشی منعطف به رعایت حریم خصوصی به‌منظور تواناسازی فناوری‌های شرکت کمک می‌کرد. در سال ۲۰۱۴ لی و همکارانش، برای بهره‌برداری از داده‌های حریم خصوصی حفاظت‌شده و کنترل دسترسی به داده‌های رمزگذاری‌شده، نوعی معماری ترکیبی ارائه کردند. کریمی و زاپاتا (۲۰۱۵) به شناسایی نوع جدیدی از حمله به حریم خصوصی و حمله‌های مختل‌کنندهٔ خدمات و سیستم‌های شرکت پرداختند و چالش‌های جدید امنیت در آیندهٔ اینترنت را بررسی کردند.

یکی از دلایل استفاده از منطق فازی در این سیستم خبره، این است که فهم و پروسه تصمیم‌گیری انسان‌ها در بسیاری از موقعیت‌ها کاملاً قطعی نیست و بسته به زمان و مکان آن، گاهی درست و گاهی نادرست است (زیدوناس و همکاران، ۲۰۰۹؛ آریانس آراندا و همکاران، ۲۰۱۰؛ اسچاتزر، ۱۹۹۰ و میا، کر و گامک، ۲۰۰۹)؛ زیرا در تفکر، استنتاج و ادراک افراد، همیشه درجهٔ معینی از فازی‌بودن وجود دارد. به‌منظور بررسی انتقادی مرتبط‌ترین پژوهش‌های پیشین با پژوهش حاضر، شرح کوتاهی از آنها در جدول ۱ به نمایش گذاشته شده است.

---

1. Privacy regulation theory

جدول ۱. بررسی انتقادی مرتبط‌ترین پژوهش‌های مبانی نظری در مقایسه با پژوهش حاضر

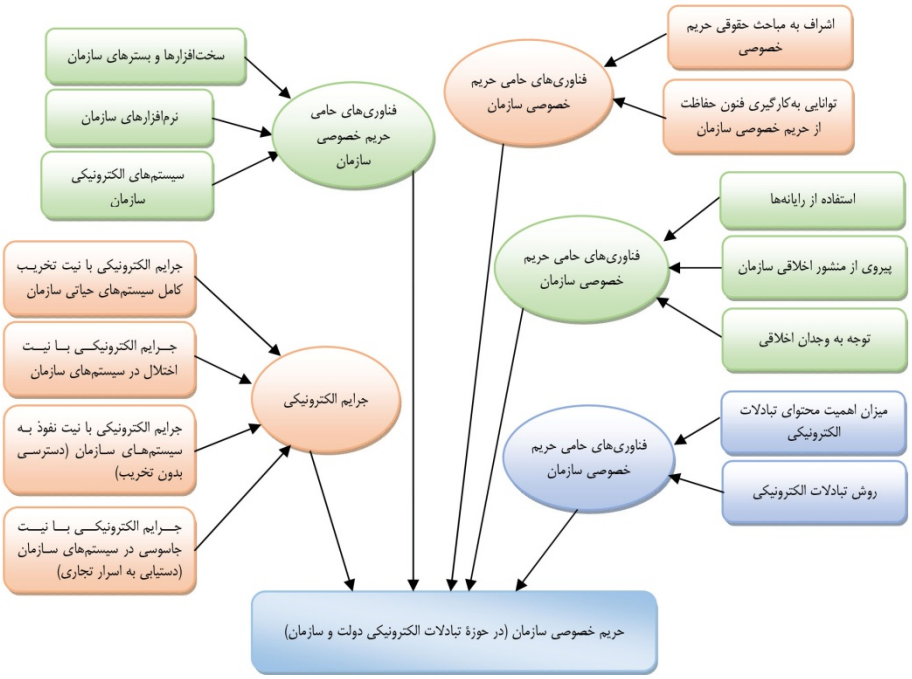
عنوان پژوهش	منبع	جنبه‌های نوآوری پژوهش										
		سیستم خبره	اعتبارسنجی سیستم	بررسی حوزهٔ امنیت		مدیر عالی حریم خصوصی	جرایم الکترونیکی	بررسی در فضای الکترونیکی	تبادلات دولت با کسب‌وکارها (G2B)	تبادلات کسب‌وکارها با دولت (B2G)	استفاده از منطق فازی	تکنیک‌ها و آزمون‌های آماری
				بررسی جزئی	بررسی مشروح							
بررسی تأثیر ادراک مشتریان از امنیت و اعتماد بر استفاده از سیستم‌های پرداخت الکترونیکی شعب بانک کشاورزی شهر تهران	کریمی، سپندارند و حق‌شناس (۱۳۹۱)	–	–	–	حفاظت فنی بر امنیت ادراک‌شدهٔ مشتریان	اعتماد تراکنش‌های الکترونیکی	اشارهٔ جزئی	سیستم پرداخت الکترونیکی	–	–	–	مدل معادلات ساختاری
بررسی تأثیر امنیت ادراک شده بر اعتماد به بانکداری اینترنتی از سوی مشتریان زن (پیمایشی دربارهٔ بانک صادرات شهر سمنان)	دامغانیان و سیاه‌سرانی کجوری (۱۳۹۱)	–	–	–	امنیت ادراک‌شدهٔ مشتریان زن بانک	اعتماد به بانکداری اینترنتی	اشارهٔ جزئی	بانکداری اینترنتی	–	–	–	مدل معادلات ساختاری
بررسی امنیت در سیستم‌های اطلاعاتی توسعه‌یافته با روش معماری سرویس‌گرا (SOA)	تقوا و ایزدی (۱۳۹۲)	–	–	–	ابعاد امنیتی سیستم‌های اطلاعاتی	–	اشارهٔ جزئی	–	–	–	–	معماری سرویس‌گرا (SOA) گردآوری داده‌ها با آزمون تی
بررسی تأثیر خصوصیات مشتریان بر تمایل آنها به پذیرش خرید اینترنتی (پیمایشی پیرامون دانشکدهٔ مدیریت دانشگاه تهران)	حسنقلی‌پور و همکاران (۱۳۹۲)	–	–	ادراکات از امنیت وب	–	نگرانی‌های حریم خصوصی	اشارهٔ جزئی	خرید اینترنتی	–	–	–	همبستگی و رگرسیون طبقه‌بندی «پترسون»
رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف	تاج‌فر و همکاران (۱۳۹۳)	–	–	–	سیستم مدیریت امنیت اطلاعات (ISMS)	محرمانه‌بودن اطلاعات سازمان	انواع جرایم الکترونیکی	–	–	–	–	رتبه‌بندی موانع ISMS برحسب اهمیت، با AHP
بررسی شاخص‌های تأثیرگذار بر موفقیت راهکارهای خدمات بانکداری نوین از دید مدیران و نخبگان بانک انصار	نادری و قاسمی‌نژاد (۱۳۹۳)	–	–	امنیت سیستم نوین بانکی	–	–	اشارهٔ جزئی	خدمات بانکداری نوین	–	–	–	رتبه‌بندی شاخص‌های تأثیرگذار بر راهکارهای خدمات نوین بانکی با تأکید بر نگرش سیستمی روش تحلیل واریانس، تحلیل عاملی اکتشافی
شناسایی تقلب در کارت‌های بانکی با استفاده از شبکه‌های عصبی مصنوعی	وثوق، تقوی‌فرد و البرزی (۱۳۹۳)	–	–	–	امنیت کارت‌های بانکی		تقلب‌های بانکی	تراکنش‌های بانکی	–	–	سیستم‌های فازی	شبکه‌های عصبی مصنوعی
An automatic search for security flaws in key management schemes	لانگلی و ریگبای (۱۹۹۲)	*	*	سیستم‌های رمزنگاری	–	–	–	شبکه‌های رایانه‌ای	–	–	–	برنامهٔ پرولوگ و مدل مبتنی بر قاعده

ادامهٔ جدول ۱

عنوان پژوهش	منبع	جنبه‌های نوآوری پژوهش									
		سیستم خبره	اعتبارسنجی سیستم	بررسی حوزهٔ امنیت		مدیر عالی حریم خصوصی	جرایم الکترونیکی	بررسی در فضای الکترونیکی	تبادلات دولت با کسب‌وکارها (G2B)	تبادلات کسب‌وکارها با دولت (B2G)	استفاده از منطق فازی	تکنیک‌ها و آزمون‌های آماری
				بررسی جزئی	بررسی مشروح							
NADIR: An automated system for detecting network intrusion and misuse.	هاچبرگ و همکاران (۱۹۹۳)	*	*	–	تعیین هویت + امنیت شبکه	–	تشخیص نفوذ	شبکه‌های رایانه‌ای	–	–	–	سیستم خبرهٔ ناهنجاری شبکه
RAMeX: a prototype expert system for computer security risk analysis and management	کایلای و جارات (۱۹۹۵)	*	*	–	مدیریت ریسک امنیت رایانه‌ای	–	تحلیل جرایم الکترونیکی	شبکه‌های بین سازمان‌های تجاری کوچک و متوسط	–	–	–	متدلوژی سیستم خبره
Grey-theory based intrusion detection model	کین و همکاران (۲۰۰۶)	*	*	–	تشخیص نفوذ به سیستم‌ها	–	اشارهٔ جزئی	سیستم‌های رایانه‌ای	–	–	–	نظریهٔ خاکستری شناسایی سریع نفوذها
A soft computing approach for privacy requirements engineering: The PriS framework	کالونیاتیس، بلسیس و گریتزالیس (۲۰۱۱)	–	*	امنیت سیستم اطلاعاتی	–	الزامات حریم خصوصی	–	سیستم‌های اطلاعاتی سازمان	–	–	استفاده از منطق فازی	ارائهٔ چارچوب مهندسی احتیاجات حریم خصوصی و امنیت
Protecting location privacy in mobile geoservices using fuzzy inference systems	هاشمی و مالک (۲۰۱۲)	*	*	–	–	حریم خصوصی	–	خدمات جغرافیایی	–	–	سیستم فازی	طراحی سیستم استنتاج فازی
Privacy-preserving data utilization in hybrid clouds.	لی و همکاران (۲۰۱۴)	–	*	داده‌های رمزگذاری	اشارهٔ جزئی	داده‌های حریم خصوصی	–	داده‌ها در محیط ابری	–	–	–	ارائهٔ معماری ترکیبی
A fuzzy anomaly detection system based on hybrid PSO-Kmeans algorithm in content-centric networks	کریمی و زاپاتا (۲۰۱۵)	*	*	–	چالش‌های جدید امنیت اینترنت	حملات به حریم خصوصی	–	امنیت در اینترنت	–	–	سیستم فازی	سیستم تشخیص ناهنجاری فازی PSO-Kmeans
Designing Fuzzy Expert System for Chief Privacy Officer (CPO) in Electronic Transactions of Government-Business (G-B) Domain	الهی، رشیدی و صادقی ۲۰۱۵ (پژوهش حاضر)	*	*	نرم‌افزارهای امنیتی شرکت	۵ مؤلفهٔ امنیت شرکت	شایستگی مدیرعالی حریم خصوصی	انواع جرایم الکترونیکی	تبادلات الکترونیکی	*	*	منطق فازی	طراحی سیستم خبرهٔ CPOFEX طراحی ابزار فازی‌کنندهٔ روابط بین مفاهیم حوزه‌های مختلف دانش ابزار اعتبارسنجی سیستم خبره

مدل مفهومی پژوهش

بر اساس ترکیب مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها، مدل مفهومی پژوهش تدوین شد (شکل ۱) که در ادامه به معرفی مؤلفه‌های آن پرداخته می‌شود.



شکل ۱. مدل مفهومی پژوهش

اخلاق مداری حرفه‌ای طرفین تبادلات الکترونیکی بین دولت و کسب‌وکارها؛ توجه اعضای شرکت و طرفین تبادلات الکترونیکی بین دولت و کسب‌وکارها به منشور اخلاقی شرکتشان و اندازهٔ پای‌بندی آنها به وجدان اخلاقی، به‌منزلهٔ بزرگ‌ترین عامل برقرارکنندهٔ عدالت اجتماعی و رعایت اصول اخلاقی در انواع تبادلات الکترونیکی بین دولت و کسب‌وکارها. سنجه‌های این مؤلفه عبارت‌اند از: خط‌مشی اخلاقی سازمان نسبت به مصرف‌کننده و مشتریان، خط‌مشی اخلاقی سازمان نسبت به پیمانکاران و مؤسسه‌های نظارتی، خط‌مشی اخلاقی سازمان نسبت به کارکنان و مدیران، توجه به وجدان اخلاقی (به‌منزلهٔ بزرگ‌ترین عامل برقرارکنندهٔ عدالت اجتماعی و کنترل‌کنندهٔ انگیزه‌های زودگذر)، توجه سازمان به استفاده از سیستم‌های

اطلاعاتی اخلاقی و خطمشی استفادهٔ اخلاقی از رایانه به‌منزلهٔ یکی از خطمشی‌های الکترونیکی سازمان (حسینی دولت‌آبادی، ۱۳۷۰ و آذر، فانی و داج‌خوش، ۱۳۹۱).

نیت جرایم الکترونیکی در حوزهٔ تبادلات الکترونیکی بین دولت و کسب‌وکارها؛ تمام تخلف‌ها و جریمه‌هایی است که با نیت خرابکاری و نابودی سیستم‌های شرکت، جاسوسی الکترونیکی و نفوذ (بدون خرابکاری) به اسرار تجاری و نقض حریم خصوصی شرکت، اخلال در سیستم‌ها و عملیات اصلی شرکت و ایجاد هرگونه مشکل برای ادامهٔ فعالیت‌های شرکت در حوزهٔ تجارت الکترونیکی، سالانه خسارت‌های مادی (کاهش فروش) و معنوی (بدنامی و صدمه به شهرت شرکت) زیادی را بر شرکت تحمیل می‌کند. به‌طور خلاصه انواع جرایم الکترونیکی عبارت‌اند از: نفوذ، گردآوری غیرمجاز داده‌ها (گردآوری داده‌های شخصی از طریق روش‌های غیرقانونی)، تغییر غیرمجاز داده‌ها (ورود به سایت و انتشار محتوای کذب)، سرقت هویت (دسترسی به شناسه و رمز عبور دیگران و وانمودکردن خود به جای آنها)، انتقال و افشای غیرمجاز داده‌ها و رعایت‌نکردن ضوابط امنیتی و سایر حقوق اشخاص حقیقی و حقوقی (اصلانی ۱۳۸۴: ۲۰۷– ۱۸۶؛ بلنگر و هیلر، ۲۰۰۶؛ بلا، گیوستولیسی و ریکوبنه، ۲۰۱۱؛ کالونیاتیس، بلسیس و گریتزالیس، ۲۰۱۱).

شایستگی مدیرعالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی بین دولت و کسب‌وکارها؛ از ترکیب مفاهیمی چون وظایف، مهارت‌ها و فنون به‌کاربرده‌شدهٔ مدیر عالی حریم خصوصی در مبانی نظری موضوع شکل گرفته است. در اینجا به بررسی توانایی مدیر عالی حریم خصوصی شرکت در به‌کارگیری فنون و روش‌های مرتبط با کار، پرداخته می‌شود (دیمیک، ۲۰۱۲ و آوازو و دسوزا، ۲۰۰۴).

فناوری‌های محافظ حریم خصوصی تبادلات الکترونیکی بین دولت و کسب‌وکارها؛ تأثیر استفاده از فناوری‌هایی مانند سیستم‌های تشخیص و جلوگیری از نفوذ، نرم‌افزارهای امنیتی، سخت‌افزارها و بسترهای مبادله‌های امن و بی‌نام و سایر ابزار الکترونیکی که شرکت برای رعایت حریم خصوصی اسرار تجاری و تبادل‌های الکترونیکی امن و بی‌نام به‌کار می‌برد. در این پژوهش به بررسی مؤلفه‌های استفاده از سیستم‌های اطلاعاتی امن (مطمئن)، سخت‌افزار و بستر پیام‌رسانی آنی رمزی، شبکه‌های پنهان‌سازی جریان اطلاعات، نرم‌افزار ضبط حرکات و کلیک‌های ماوس و صفحهٔ کلید، فناوری متوقف‌کردن سایت‌های شخص ثالث ردیاب در سراسر وب، گذرواژه‌های یک‌بار مصرف، فناوری‌های حفاظت از حریم خصوصی انتشار و ثبت‌کردن اطلاعات حساس سازمان، فناوری پیام خودانهدام متنی، صوتی و تصویری (به‌منظور حفاظت از

حریم خصوصی ابزار موبایل سازمان) پرداخته شده است (کایلای و جارات، ۱۹۹۵؛ سامرز، استنلی و کوزبان، ۱۹۹۸ و هاچبرگ و همکاران، ۱۹۹۳).

نوع تبادلات الکترونیکی بین دولت و کسب‌وکارها؛ میزان خطرپذیری و ریسک تبادل الکترونیکی بین دولت و کسب‌وکارها، از طریق درگاه‌های دولتی و سایر روش‌های تبادل الکترونیکی بین دولت و کسب‌وکارها است. در پژوهش پیش رو، سنجه‌هایی چون فرمول‌ها، تألیفات منتشرنشده و طرح‌های تجاری و نیز نرم‌افزارها، فرایندها و روش‌های تجارت شرکت، محتوای تبادلات درنظر گرفته شدند و به بررسی مبادلهٔ الکترونیکی از طریق وب‌سایت، رایانامه، تلفن و ... پرداخته شده است (بلا، گیوستولیسی و ریکوبنه، ۲۰۱۱؛ ردیک و روی، ۲۰۱۳ و دینو و هارت، ۲۰۰۶).

روش‌شناسی پژوهش

از آنجا که تحقیقات طراحی، به روش‌شناسی منحصربه‌فردی نیاز دارد، در این مقاله با بررسی پارادایم‌های اصلی زیربنای فلسفی پژوهش‌های علوم اجتماعی و مدیریت و روش پژوهش سیستم‌های اطلاعاتی، از ترکیب نظریهٔ انتقادی و رویکرد پژوهشی علم طراحی[1] استفاده شده است. در واقع از دید هستی‌شناسی ـ پارادایم پژوهشی انتقادی، در این مقاله واقعیت و مسائلی که مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها با آنها سروکار دارد را هاله‌ای از عوامل اجتماعی، سیاسی، فرهنگی، اقتصادی، اخلاقی و... احاطه کرده است که این عوامل تأثیرگذار بر تصمیم‌های مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها، در گذر زمان و در صورت تعامل با اعضای شرکت، شفاف می‌شوند. در واقع این پژوهش از نظر ماهیت، کاربردی است؛ زیرا نتایج و یافته‌های آن برای حل مسائل مختص به مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها که یکی از مشکلات خاص سازمان‌ها به‌شمار می‌رود، به‌کار برده می‌شود. از دید شناخت‌شناسی، پژوهشگر به بررسی جامع پدیدهٔ مد نظر به شیوه‌ای تعاملی با خبرگان این حوزه اقدام می‌کند و خبرگان نیز نظرشان را دربارهٔ درستی و ارتباط مفاهیم و قواعد پرسشنامه بیان می‌کنند. در اینجا ذهنیت‌گرایی و ارزش‌های خبرگان حوزهٔ مطالعه، بر پدیده تأثیر می‌گذارد. شناخت‌شناسی در رویکرد پژوهشی علم طراحی این مقاله به دو مسئله اشاره می‌کند؛ یکی دانستن از طریق ساختن سیستم خبره و دیگری سازه‌های عینی محدود درون مضمون حریم خصوصی. از دید ارزش‌شناسی، به خلق دانش جدید دربارهٔ حوزهٔ کاری مدیر عالی حریم خصوصی، پیشرفت و بهبود در وضعیت حریم

1. Design Science

خصوصی تبادلات الکترونیکی بین دولت و کسب‌وکارها و فهم مسائل کاری مدیر عالی حریم خصوصی پرداخته شده است (وایشناوی و کوچلر، ۲۰۰۸: ۲۰-۱۴ و کاتز، ۲۰۰۶: ۳۰۴- ۳۰۲). در واقع روش اجرای این پژوهش از نظر هدف، توصیفی ـ ارزشیابی است؛ زیرا از سویی اقدام به توصیف دقیق مفاهیم و قواعد حوزهٔ مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها می‌پردازد و از سوی دیگر، روابط بین این مفاهیم و قواعد را با استفاده از پرسشنامه و مصاحبه با خبرگان ارزیابی و تعیین می‌کند. در واقع روش نمونه‌گیری در این مقاله ترکیبی از دو روش نمونه‌گیری غیر احتمالی هدفمند و نمونه‌گیری گلولهٔ برفی است. گفتنی است، حجم نمونهٔ این پژوهش را سه گروه معرفی‌شده از خبرگان در دسترس و مایل به همکاری در جامعهٔ آماری شکل می‌دهد. برای دستیابی به مدل، از اسناد موجود در مجله‌های مرتبط با کار مدیر عالی حریم خصوصی در حوزهٔ کسب‌وکار الکترونیکی، توصیه‌های سازمان توسعهٔ همکاری‌های اقتصادی (OECD)، هشدارهای پلیس بین‌الملل دربارهٔ حریم خصوصی در فضای الکترونیکی، مرکز اطلاعاتی حریم خصوصی الکترونیکی (EPIC) و قانون تجارت الکترونیکی ایران، استفاده شده است. به‌منظور ارزیابی مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها، از نظر ۱۷۲ نفر از متخصصان دانشگاهی، از جمله استادان حقوق دانشگاه‌های تربیت مدرس و شهید بهشتی، مرکز تحقیقات صنایع انفورماتیک و همچنین متخصصان بخش دولتی مانند پلیس فتا (فضای تبادل اطلاعات)، معاونت امنیت فضای تبادل اطلاعات وزارت ارتباطات و فناوری اطلاعات و... بهره برده شد. داده‌های پرسشنامهٔ اول در فاصلهٔ زمانی شهریور ۱۳۹۳ تا آبان ۱۳۹۳ و داده‌های پرسشنامهٔ دوم در آذرماه ۱۳۹۳ جمع‌آوری شده است. ضریب آلفای کرونباخ ۹۳ گزینهٔ پرسشنامه برای پایایی مؤلفه‌های تعیین‌کنندهٔ وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، ۰/۷۳ به‌دست آمد که قابلیت اعتماد بالای پرسشنامه را نشان می‌دهد.

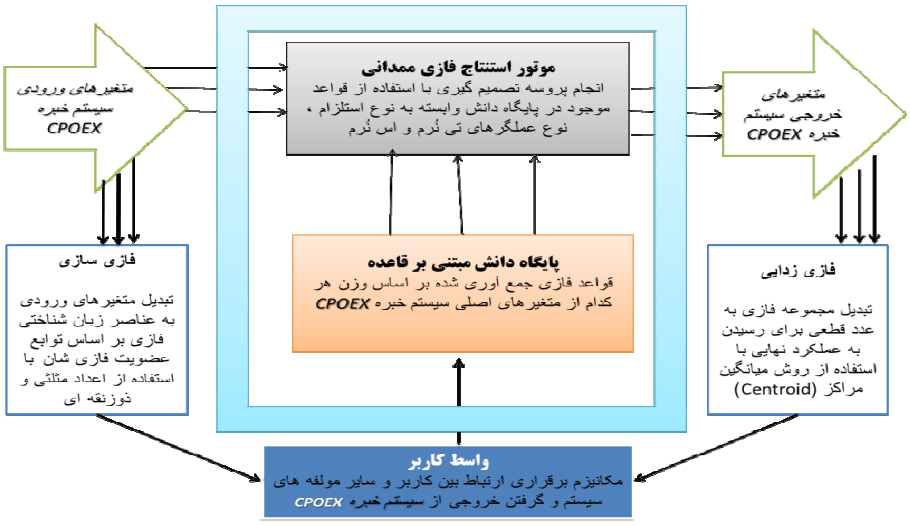
یافته‌های پژوهش و طراحی سیستم خبرهٔ فازی

در این پژوهش سیستم خبره در پنج مرحله طراحی شده است که عبارت‌اند از: فازی‌سازی، پایگاه قواعد فازی، موتور استنتاج فازی و غیرفازی‌سازی و اعتبارسنجی سیستم خبرهٔ طراحی‌شده. با توجه به تحلیل ساختار سیستم‌های خبرهٔ به‌کاررفته در مجله‌های معتبر در حوزهٔ سیستم‌های خبره[1] (ژو و همکاران، ۲۰۰۷؛ لی بلنک و جلاسی، ۱۹۹۱؛ لیائو، ۲۰۰۵ و ژیدوناس و همکاران،

1. Expert System With Applications

۲۰۰۹)، اجزای ساختار سیستم خبرهٔ این پژوهش طراحی شد که در شکل ۲ به نمـایش گذاشـته شده است.

فازی‌سازی: بعد از طراحی مدل مفهومی پـژوهش، بـه تعریـف متغیـرهـای ورودی و خروجـی سیستم خبره اقدام می‌شود. در واقع ماژول «وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها»، خروجی سیستم خبرهٔ پیشنهادی را شکل می‌دهد. جدول ۲ افرازبندی متغیـرهـای زبانی مرتبط با متغیر خروجی سیستم خبرهٔ پژوهش را بر اساس نظر خبرگان به نمـایش گذاشـته است.



شکل ۲. ساختار پیشنهادی سیستم خبرهٔ پژوهش حاضر

جدول ۲. متغیرهای زبانی مرتبط با وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها

شماره	متغیر زبانی	معادل انگلیسی	علامت اختصاری	توابع عضویت اعداد مثلثی و ذوزنقه‌ای
۱	نا امن	InSecure	Worst	(۰/۱۵, ۰/۰۳, ۰, ۰)
۲	ریسک زیاد	High Risk	H-R	(۰/۳, ۰/۲, ۰/۱)
۳	ریسک متوسط	Medium Risk	M-R	(۰/۷, ۰/۵, ۰/۳)
۴	کم‌ریسک	Low Risk	L-R	(۰/۹, ۰/۸, ۰/۷)
۵	امن	Secure	Best	(۱, ۱, ۰/۹۷ ۰/۸۵)

پایگاه قواعد فازی: پایگاه قواعد فازی مجموعه‌ای از قواعد اگر ـ آنگاه است که قلب سیستم خبرهٔ این پژوهش به‌شمار می‌رود. در اینجا احتمال وقوع حالت‌های مختلف بین متغیرهای اصلی سیستم خبره، یکسان در نظر گرفته شده است. نحوهٔ تولید قواعد پایگاه دانش ماژول اصلی سیستم خبره (وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها) به شرح زیر است:

محاسبهٔ وزن هریک از متغیرهای اصلی با بهره‌مندی از نظر خبرگان: با توجه به جدول وزن نهایی متغیرهای اندازه‌گیری‌کننده، وزن هر یک از متغیرهای اصلی به‌دست آمد که در جدول ۳ مشاهده می‌شود.

جدول ۳. وزن هر یک از متغیرهای اصلی پژوهش

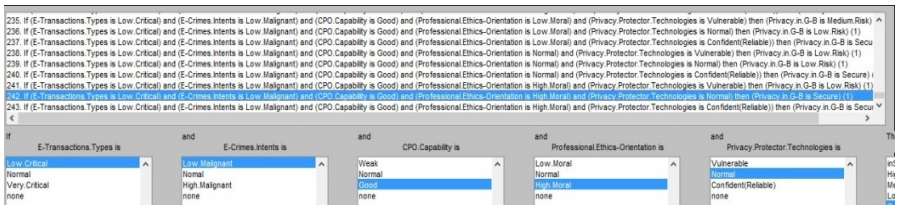
شماره	متغیر اصلی	سنجه‌ها	وزن نهایی متغیر
۱	اخلاق‌مداری حرفه‌ای طرفین تبادلات الکترونیکی	۷	۰/۸۱۱
۲	شایستگی مدیر عالی حریم خصوصی شرکت	۲۸	۰/۷۷۹
۳	نوع تبادلات الکترونیکی دولت و کسب‌وکارها	۲۴	۰/۷۷۲
۴	فناوری‌های حافظ حریم خصوصی شرکت	۱۷	۰/۷۷۱
۵	نیت جرایم الکترونیکی	۱۷	۰/۷۶۸

محاسبهٔ مقدار متغیر خروجی بر اساس وزن هریک از متغیرها: با توجه به وزن هر یک از پنج متغیر اصلی سیستم خبره، می‌توان وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها را در حالت‌های مختلف بررسی کرد. جدول ۴ نحوهٔ محاسبهٔ وزن حالت‌های ممکن برای تولید قاعده در پایگاه دانش سیستم خبره را نشان می‌دهد.

با توجه به توابع عضویت متغیرهای زبانی خبرگان، ۰/۲۴۷۶۳۶ در بازهٔ تعریف‌شده برای متغیر زبانی «ریسک زیاد» جانمایی شده است. از این رو، وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها در حالت بالا (جدول ۴) در «ریسک زیاد» قرار دارد. سایر قواعد پایگاه دانش این سیستم خبره نیز به این ترتیب تولید شدند و در پرسشنامه‌ای به مقایسهٔ پاسخ‌های سیستم خبره با میانگین نظر خبرگان پرداخته شد. شکل ۳ نحوهٔ تولید قواعد پایگاه دانش ماژول اصلی سیستم خبره را نشان می‌دهد.

جدول ٤. نحوهٔ محاسبهٔ وزن حالت‌های ممکن برای تولید قاعده در پایگاه دانش سیستم خبره

حالت‌های ممکن برای تولید قاعده	تأثیر بر متغیر خروجی	وزن متغیر × مقدار قطعی متغیر	وزن حالت مفروض
اگر «نیت جرائم الکترونیکی» با بد خواهی زیاد باشد.	رابطهٔ منفی	۰/۰۲۵ × ۰/۷۶۸	۰/۰۱۹۲
و «شایستگی مدیرعالی حریم‌خصوصی» در وضعیت معمولی باشد.	رابطهٔ مثبت	۰/۵ × ۰/۷۷۹	۰/۳۸۹۳
و «اخلاق‌مداری حرفه‌ای طرفین تبادلات الکترونیکی» زیاد باشد.	رابطهٔ مثبت	۰/۹۷۵ ×۰/۸۱۱	۰/۷۹۱۱
و «نوع تبادلات الکترونیکی دولت و کسب‌وکارها» خیلی مهم باشد.	رابطهٔ منفی	۰/۰۲۵ × ۰/۷۷۲	۰/۰۱۹۳
و «فناوری‌های محافظ حریم خصوصی شرکت» ضعیف باشند.	رابطهٔ مثبت	۰/۰۲۵ × ۰/۷۷۱	۰/۰۱۹۳
آنگاه: حریم‌خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها در چه وضعیتی قرار دارد؟	میانگین وزن حالت‌های مفروض: ۰/۰۱۹۲۹۷۶۲۵ + ۰/۷۹۱۱۴۳۲۷۵ + ۰/۳۸۹۲۶۸۵ + ۰/۰۱۹۱۹۷۳۷۵ + ۰/۰۱۹۲۷۱۷۵ ۰/۲۴۷۶۳۶ ÷ ۵ =۱/۲۳۸۱۷۹		

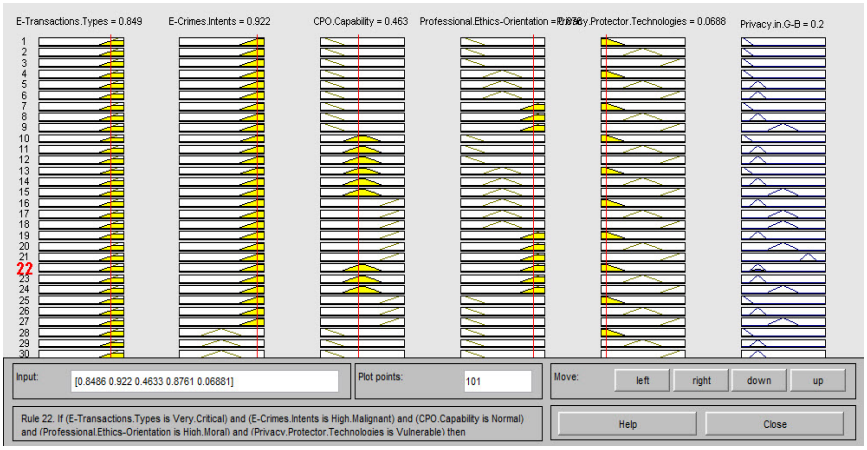


شکل ۳. نحوهٔ تولید قواعد پایگاه دانش ماژول اصلی سیستم خبره

موتور استنتاج فازی: در بخش جعبهٔ فازی نرم‌افزار متلب، به‌منظور اتصال قواعد فازی سیستم با استفاده از عملگر «و» و «Sum»، سبک تجمیع قواعد فازی[1] انتخاب شده است. بدین ترتیب، مجموع دقیق‌تر هر مجموعهٔ خروجی قواعد در نظر گرفته می‌شود، نه حداکثر آنها. دلیل اصلی استفاده از سیستم استنتاج فازی ممدانی این است که موتور استنتاج فازی ممدانی، معایب سیستم فازی خالص و سیستم فازی سوگنو را برطرف کرده است، ضمن آنکه یک فازی‌ساز در ورودی و یک غیرفازی‌ساز در خروجی سیستم قرار می‌دهد. برای انتخاب نوع استلزام در نرم‌افزار متلب از Prod استفاده می‌شود؛ زیرا عملگر مینیمم مجموعهٔ فازی خروجی را کوتاه و ناقص می‌کند. در واقع دلیل استفاده از Prod، مقیاس‌بندی دقیق‌تر خروجی مجموعه‌های فازی است (سیوناندام،

1. Aggregation

سوماتی و دیپا، ۲۰۰۷: ۱۲۷– ۱۱۳). غیرفازی‌ساز، خروجی فازی را به عدد قطعی تبدیل می‌کند. در قسمت غیرفازی‌ساز نرم‌افزار متلب، روش Centroid انتخاب می‌شود. شکل ۴ نمایی از تحلیل رفتار متغیر خروجی در ماژول وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، به‌صورت عددی و زبانی، بر اساس پنج متغیر اصلی سیستم خبره را نشان می‌دهد.



شکل ٤. تحلیل رفتار متغیر وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها

ارزیابی نهایی پاسخ‌های سیستم خبره: بعد از طراحی سیستم خبرهٔ پژوهش با انتخاب تصادفی ۱۰ قاعده از سیستم خبره، خروجی‌های سیستم خبره در پرسشنامهٔ جداگانه‌ای (جدول ۵) با نظر ۱۸ نفر از خبرگان مقایسه شد. همان‌طور که در جدول ۶ مشاهده می‌شود، اختلاف نهایی بین خروجی‌های سیستم خبره و میانگین نظر خبرگان معنادار نیست (۰/۰۶۴۷۵). این نتیجه نشان می‌دهد سیستم خبرهٔ فازی مدیر عالی حریم خصوصی، از اعتبار کافی برخوردار است.

جدول ۵. ابزار اعتبارسنجی سیستم خبره از طریق مقایسهٔ پاسخ‌ها با نظر خبرگان

شمارهٔ قاعده	متغیرهای ورودی سیستم خبره					متغیر خروجی سیستم خبره	نظر شما
	الف	ب	ج	د	ه	و	
۳	زیاد	کم	کم	زیاد	زیاد	؟	
...							

الف: نیت جرایم الکترونیکی
ب: شایستگی مدیر عالی حریم‌خصوصی
ج: اخلاق‌مداری حرفه‌ای
د: نوع تبادلات الکترونیکی
ه: فناوری‌های محافظ حریم خصوصی
و: حریم‌خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها

جدول ٦. نظر خبرگان دربارهٔ وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها

شمارهٔ قاعده	میانگین پاسخ‌های خبرگان	خروجی‌های سیستم خبره	اختلاف پاسخ‌ها بر اساس مقیاس پنج‌تایی	میانگین اختلاف‌ها
۳	۱/۲۲	۱	۰/۰۵۵ = ۴ / ۰/۲۲	
۴۵	۲/۷۲	۳	۰/۰۶۷۵ = ۴ / ۰/۲۸	
۷۹	۲/۷۸	۳	۰/۰۵۵ = ۴ / ۰/۲۲	
۸۶	۱/۶۷	۲	۰/۰۸۲۵ = ۴ / ۰/۲۲	
۱۰۳	۱/۶۷	۲	۰/۰۸۲۵ = ۴ / ۰/۲۲	۰/۰۶۴۷۵
۱۴۰	۲/۷۸	۳	۰/۰۵۵ = ۴ / ۰/۲۲	
۱۵۷	۳	۳	۰ = ۴ / ۰	
۲۱۹	۲/۹۴	۳	۰/۰۱۵ = ۴ / ۰/۰۶	
۲۲۴	۳/۳۹	۴	۰/۱۵۲۵ = ۴ / ۰/۶۱	
۲۳۵	۲/۶۷	۳	۰/۰۸۲۵ = ۴ / ۰/۲۲	

مقایسهٔ یافته‌ها: به‌منظور مقایسهٔ نتایج مرتبط‌ترین پژوهش‌های مبانی نظری با یافته‌های پژوهش حاضر، شرح مختصری از آنها در جدول ۱ به نمایش گذاشته شد. پژوهش‌های مندرج در جدول ۱ بر اساس این جنبه‌ها بررسی و مقایسه شدند: طراحی سیستم خبره، اعتبارسنجی سیستم، بررسی حوزهٔ امنیت، بررسی فنون به‌کاررفتهٔ مدیر عالی حریم خصوصی، شناسایی جرایم الکترونیکی مرتبط با حوزه، بررسی در فضای الکترونیکی، تبادلات دولت با کسب‌وکارها (G2B)، تبادلات کسب‌وکارها با دولت (B2G) و استفاده از منطق فازی. نتایج مقایسه‌های جدول ۱ ضمن کمک به شناسایی شکاف‌های این حوزه، نشان می‌دهد یافته‌های پژوهش حاضر، بخشی از کاستی‌های پژوهش‌های پیشین در این حوزه را رفع می‌کند.

نتیجه‌گیری و پیشنهادها

نوع و میزان ارتباط مفاهیم کار مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها، تابع منطق فازی است؛ زیرا عوامل بسیاری در فرایند انتخاب و به‌کارگیری فناوری‌ها، روش‌ها و نظریه‌های به‌کاربرده‌شدهٔ وی تأثیر می‌گذارند که هر یک از این عوامل از ابهام و پیچیدگی بسیاری برخوردارند. مهم‌ترین نتیجهٔ این پژوهش را می‌توان تحلیل وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها، بر اساس مؤلفه‌های شایستگی مدیر عالی حریم خصوصی، نیت جرایم الکترونیکی، نوع تبادلات الکترونیکی دولت و کسب‌وکارها، اخلاق‌مداری حرفه‌ای طرفین تبادلات الکترونیکی و فناوری‌های محافظ حریم خصوصی شرکت،

بیان کرد. با توجه به بررسی پایگاه‌های اطلاعاتی اسکوپوس، اشپرینگر، ساینس دایرکت، ایران داک و غیره، می‌توان برخی از جنبه‌های نوآوری این مقاله را به این شرح بیان کرد: ۱. طراحی سیستم خبره برای مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها بر اساس مهم‌ترین نرم‌افزارها؛ ۲. روش‌ها و جرایم فضای کسب‌وکار الکترونیکی؛ ۳. شناسایی مفاهیم مرتبط با کار مدیر عالی حریم خصوصی در حوزهٔ تبادلات الکترونیکی دولت و کسب‌وکارها و مدل‌سازی جامع پایگاه دانش سیستم خبره بر اساس آنها؛ ۴. استفاده از رویکرد منطق فازی به‌منظور ارائهٔ توصیه‌هایی دقیق‌تر دربارهٔ وضعیت حریم خصوصی تبادلات الکترونیکی دولت و کسب‌وکارها.

در پایان می‌توان گفت، سازمان‌هایی که با نهادها و سازمان‌های دولتی تبادلات الکترونیکی دارند، می‌توانند با استفاده از سیستم خبرهٔ طراحی‌شدهٔ این پژوهش، وضعیت حریم خصوصی تبادلات الکترونیکی بین دولت و سازمان‌شان را بررسی و ارزیابی کنند و با توجه به رویکرد جامع مدل این سیستم، ریسک تبادلات الکترونیکی را مدیریت کنند. به‌علاوه، به‌کارگیری سیستم خبرهٔ این پژوهش در سازمان‌های فعال در حوزهٔ امنیت اطلاعات و ارتباطات، می‌تواند به کاهش هزینهٔ کسب تجربهٔ کاربران سازمانی کمک کند؛ زیرا سیستم‌های خبره دائمی و پایدارند و مانند انسان‌های خبره نمی‌میرند و فناناپذیرند. یکی دیگر از مزیت‌های این سیستم، سهولت انتقال آن به مکان‌های جغرافیایی گوناگون است. این امر برای توسعهٔ کشورهایی که استطاعت خرید دانش متخصصان را ندارند، بسیار اهمیت دارد و در کاهش هزینه‌های آنها مؤثر است. با توجه به مطالب بیان‌شده، مهم‌ترین توصیه و پیشنهاد برای پژوهش‌های بعدی را می‌توان، ادغام سیستم خبرهٔ این پژوهش با روش‌های هوش مصنوعی، به‌ویژه شبکهٔ عصبی مصنوعی و الگوریتم‌های حوزهٔ هوش مصنوعی برای افزایش غنای محتوای سیستم خبرهٔ یادشده و بهبود فرایند استنتاج فازی آن، بیان کرد.

References

Arias-Aranda, D., Castro, J.L., Navarro, M., Sánchez, J.M., Zurita, J.M. (2010). A Fuzzy expert system for business management. *Expert Systems with Applications*, 37 (12): 7570–7580.

Aslani, H.R. (2006). Information Technology Laws. Tehran: Mizan Publications. (*in Persian*)

Awazu, Y. & Desouza, K. C. (2004). The Knowledge Chiefs: CKOs, CLOs and CPOs. *European Management Journal*, 22(3): 339–344.

Bamberger, K.A. & Mulligan, D.K. (2011). New governance, chief privacy officers, and the corporate management of information privacy in the United States: An initial inquiry. *Law & Policy*, 33(4): 477-508.

Belanger, F. & Hiller, J.S. (2006). A framework for e-government: privacy implications. *Business process management journal,* 12 (1): 48-60.

Beldad, A., de Jong, M. & Steehouder, M. (2010). Reading the least read? Indicators of users' intention to consult privacy statements on municipal websites. *Government Information Quarterly*, 27(3): 238-244.

Bella, G., Giustolisi, R. & Riccobene, S. (2011). Enforcing privacy in e-commerce by balancing anonymity and trust. *Computers & Security*, 30 (8): 705-718.

Damghanian, H. & Siahsarani Kojuri, M. A. (2012). A Study on the Effect of Perceived Security on the Trust of Female Customers in the Internet Banking: (A Survey of the SADERAT BANK in Semnan). *Journal of Information Technology Management*, 4(13): 71-88. (*in Persian*)

Den Butter, F. A. G., Liu, J., & Tan, Y.H. (2012). Using IT to engender trust in government-to-business relationships: The Authorized Economic Operator as an example. *Government Information Quarterly*, 29(2): 261-274.

Dimick, C. (2012). The new privacy officer. *Journal of AHIMA/American Health Information Management Association*, 83(4): 20-25.

Dinev, T. & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research*, 17 (1): 61-80.

Elahi, Sh. & Hassanzadeh, A. (2009). A framework for evaluating electronic commerce adoption in Iranian companies. *International Journal of Information Management*, 29(1): 27–36.

Ghodselahi, A. (2011). *Designing a Fuzzy Expert system for Risk Management in Banking Industry.* [Master thesis]. Supervisor: Elahi, Sha'ban. Tehran: Tarbiat Modares University, Faculty of Management and Economic. (*in Persian*)

Hasangholipour, T., Amiri, M., Fahim, F.S. & Ghaderi Abed, A. (2013). Effects of Consumer Characteristics on their Acceptance of Online Shopping: A Survey in Faculty of Management, University of Tehran. *Journal of Information Technology Management*, 5(4): 67-84. (*in Persian*)

Hashemi, M. & Malek, M.R. (2012). Protecting location privacy in mobile geoservices using Fuzzy inference systems. Computers. *Environment and Urban Systems*, 36(4): 311–320.

Hochberg, J., Jackson, K., Stallings, C., McClary, J.F., DuBois, D. & Ford, J. (1993). NADIR: An automated system for detecting network intrusion and misuse. *Computers & Security*, 12(3): 235-248.

Hosseini Dolwlat Abadi, F. (2001). *The Ethical Conscience and ways of fostering it.* [Master thesis]. Supervisor: Dr Hojati. Tehran: Tarbiat Modares Uni. (*in Persian*)

Jensen, C., Potts, C. & Jensen, C. (2005). Privacy practices of Internet users: Self-reports versus observed behavior. *International Journal of Human-Computer Studies*, 63(1–2): 203–227.

Jutla, D.N., Bodorik, P. & Zhang, Y. (2006). PeCAN: An architecture for users' privacy-aware electronic commerce contexts on the semantic web. *Information Systems*, 31 (4): 295-320.

Kailay, M. P. & Peter, J. (1995). RAMeX: a prototype expert system for computer security risk analysis and management. *Computers & Security*, 14(5): 449–463.

Kalloniatis, Ch., Belsis, P. & Gritzalis, S. (2011). A soft computing approach for privacy requirements engineering: The Pris framework. *Applied Soft Computing*, 11(7): 4341–4348.

Karami, A. & Guerrero-Zapatab, M. (2015). A Fuzzy anomaly detection system based on hybrid PSO-Kmeans algorithm in content-centric networks. *Neurocomputing,* 149: 1253–1269.

Karat, J., Karat, C.M., Brodie, C. & Feng, J. (2005). Privacy in information technology: Designing to enable privacy policy management in organizations. *International Journal of Human-Computer Studies,* 63(1): 153-174.

Le Blanc, L. A. & Jelassi, T. (1991). an evaluation and selection methodology for expert system shells. *Expert Systems with Applications*, 2(2–3): 201–209.

Li, J., Li, J., Chen, X., Liu, Zh. & Jia, CH. (2014). Privacy-preserving data utilization in hybrid clouds. *Future Generation Computer Systems*. (30): 98–106.

Liao, SH. (2005). Expert system methodologies and applications-a decade review from 1995 to 2004. *Expert Systems with Applications*, 28 (1): 93-103.

Longley, D. & Rigby, S. (1992). An automatic search for security flaws in key management schemes. *Computers & Security*. 11(1): 75-89.

Majdalawieh, M. (2010). The Integrated Privacy Model: Building a Privacy Model in the Business Processes of the Enterprise. *International Journal of Information Security and Privacy archive*, 4 (3): 1-21.

Miah, Sh., Kerr, D. & Gammack, J.G. (2009). A methodology to allow rural extension professionals to build target-specific expert systems for Australian rural business operators. *Expert Systems with Applications*. 36(1): 735–744.

Naderi, A & Ghaseminezhad, Y. (2014). Investigating the Indicators Affecting the Success of Modern Banking Services Strategies from the View Point of Managers and Experts of Ansar Bank. *Journal of Iranian Technology Management*, 6(3): 487-504.

Qin, B., Zhou, X., Yang, J. & Song, C. (2006). Grey-theory based intrusion detection model. *Journal of Systems Engineering and Electronics*, 17(1): 230–235.

Reddick, C.G. & Roy, J. (2013). Business perceptions and satisfaction with e-government: Findings from a Canadian. *Government Information Quarterly*, 30(1): 1-9.

Reza Karimi, M., Sepandarand, S. & Haghshenas, F. (2012). Study of the Effects of Customers' Perceptions of Security and Trust on their Use of the Agriculture Bank of Iran's e-Payment System. *Journal of Iranian Technology Management*, 4(11): 135-154.

Rezmierski, V. E. & Marshall, R. S. (2002). University systems security logging: who is doing it and how far can they go? *Computers & Security*, 21 (6)1: 557–564.

Shamsi, Z. (2014). *Designing a Fuzzy expert system for selecting new IT product development projects*. [Master thesis]. Supervisor: Elahi, Sha'ban. Tehran: Tarbiat Modares University, Faculty of Management and Economic. (*in Persian*)

Sivanandam, S. N., Sumathi, S. & Deepa, S.N. (2007). *Introduction to Fuzzy Logic using MATLAB*. Springer-Verlag Berlin Heidelberg.

Summers, R. C. & Kurzban, S.A. (1988). Potential applications of knowledge-based methods to computer security. *Computers & Security*, 7(4): 373–385.

Taghva, M.R. & Izadi, M. (2013). Investigating Security in Developed Information Systems through Service oriented Architecture (SOA). *Journal of Information Technology Management*, 5(3): 25-42. (*in Persian*)

Tajfar, A. H., Mahmoudi Maymand, M., Rezasoltani, F. & Rezasoltani, P. (2015). Ranking the barriers of implementing Information Security Management

System and Investigation of readiness rate of exploration management. *Journal of Information Technology Management*, 6(4): 551-566. (*in Persian*)

Vaishnavi, V. K. & Kuechler, Jr. W. (2008). *Design Science Research Methods and Patterns, Innovating Information and Communication Technology*. Auerbach Publications, Taylor & Francis Group.

Vosough, M., Taghavi Fard, M. T. & Alborzi, M. (2015). Bank card fraud detection using artificial neural network. *Journal of Information Technology Management*, 6(4): 721-746. (*in Persian*)

Xidonas, P., Ergazakis, E., Ergazakis, K., Metaxiotis, K., Askounis, D., Mavrotas, G. & Psarras, J. (2009). On the selection of equity securities: An expert systems methodology and an application on the Athens Stock Exchange. *Expert Systems with Applications*, 36(9): 11966–11980.

Xu, D.L., Liu, J., Yang, J.B., Liu, G.P., Wang, J., Jenkinson, I. & Ren, J. (2007). Inference and learning methodology of belief-rule-based expert system for pipeline leak detection. *Expert Systems with Application*, 32(1): 103-113.