Journal iranian political sociology

Vol. ۵, No.۱۰, dey ۲۰۲۲

Exploring the Information Security Management Model in Iranian Government Organizations with an Organized Crime Prevention Approach

The main action to create security in an organization is to create a strong body for information security management. Information security management provides a model for protecting an organization's information assets, thereby minimizing the possibility of unauthorized access to these sensitive assets. Experts believe that attacks such as fraud, information theft and money laundering, which are routinely conducted online, along with other crimes such as computer theft, computer fraud, cyber espionage and information disclosure, are all organized crimes. The context of crisis and crime, the adoption of appropriate policies and preventive management has become more necessary than ever, so the present qualitative research with the ultimate goal of "exploring the pattern of information security management in Iranian government organizations with an organized crime prevention approach" and Using the research method of data foundation theory, interview data collection method, theoretical sampling and interviews, theoretical saturation was obtained. A collection of ۱۷snowball were performed and with basic themes was collected during the open coding process and categories were extracted from them. Then, in the axial coding stage, the links between these categories were determined in the form of a coding paradigm. Then, in the selective coding stage, each component of the coding paradigm was described, the .course of the drawing and the pattern were created

ماهنامه علمی (مقاله علمی_پژوهشی) جامعه شناسی سیاسی ایران، سال پنجم،شماره ده، دی۱٤۰۱،صص۳٤۳۸-۳٤۲۱

کاوش الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته و تبیین جامعه شناختی آن

حجت طالبی[۱]
حمید تابلی[۲]
محمد ضیاءالدینی[۳]
رضا فخر طاولی[٤]

تاریخ دریافت : ۱۳۹۹/۱۲/۱٤
تاریخ پذیرش: ۱٤۰۱/۰۷/۰۵

چکیده

اصلی‌ترین اقدام برای ایجاد امنیت در یک سازمان، ایجاد یک بدنه قوی در راستای مدیریت امنیت اطلاعات است. مدیریت امنیت اطاعات مدلی را به منظور حفاظت از دارایی‌های اطلاعاتی سازمان ارائه می‌کند که در نتیجه آن احتمال دسترسی غیر مجاز به این دارایی‌های حساس به حداقل می‌رسد. صاحب‌نظران معتقدند حملاتی از قبیل کلاهبرداری، دزدی اطلاعات و پولشویی که امروزه به صورت اینترنتی هدایت می شوند در کنار جرایم دیگری چون سرقت رایانه ای، جعل رایانه‌ای، جاسوسی اینترنتی و افشای اطلاعات همگی در زمره جرایم سازمان یافته هستند لذا در این بستر بحران زا و جرم زا، اتخاذ سیاستهای مناسب و مدیریت پیشگیرانه بیش از پیش ضرورت یافته است، از این رو پژوهش کیفی حاضر با هدف غایی " کاوش الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته" و با استفاده از روش تحقیق نظریه داده بنیاد، روش جمع‌آوری داده مصاحبه، نمونه‌گیری نظری و گلوله برفی انجام و با ۱۷ مصاحبه اشباع نظری آن حاصل شد. در ادامه و در مرحله کدگذاری گزینشی، یکایک اجزای پارادایم کدگذاری تشریح، سیر فعالیت ترسیم و الگو خلق شد.

واژگان کلیدی: مدیریت امنیت اطلاعات، امنیت داده، جرائم سازمان یافته، سازمان‌های دولتی.

[۱]دانشجوی دکتری مدیریت دولتی، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران.
[۲]دانشیار گروه مدیریت دولتی، دانشگاه پیام نور، تهران، ایران .
[۳]استادیار گروه مدیریت دولتی، واحد رفسنجان، دانشگاه آزاد اسلامی، رفسنجان، ایران.
[٤]استادیار گروه کامپیوتر، واحد چالوس، دانشگاه آزاد اسلامی، چالوس، ایران.

۱- مقدمه

اطلاعات در دنیای کنونی ارزشمندترین دارایی هر سازمان محسوب می‌شود و باید آن را کالای اساسی هر سازمان دانست. در عصر جدید، اطلاعات و ارتباطات و دو عنصر سازنده قدرت هستند(خواجه سروری و خجسته،۱۳۹۸). اطلاعات مهمترین گنجینه سازمان‌ها و اشخاص می‌باشد که از بین رفتن و حتی کوچک‌ترین آسیب به آن، نیازمند صرف زمان، هزینه و نیروی کار تصور ناپذیری برای جبران است و در برخی مواقع اصول کاری و موجودیت یک سازمان را تهدید می‌کند (موسوی و حسن‌پور،۱۳۹٤). حیات سازمان‌ها ارتباط نزدیکی با سیستم اطلاعاتی آن‌ها دارد (تاج‌فر،۱۳۹۳) لذا توجه به این نکته که سیستم امنیتی نامطلوب در بیشتر موارد، علت وقوع جرم است، ضروری به نظر می رسد(وروایی و میرزکی،۱۳۹۰). چون سازمان‌ها، بسیاری از منابع و امتیازات‌شان را از محیط اطراف کسب می‌کنند، چنانچه نتوانند امنیت اطلاعات سازمان و یا افراد مرتبط با سازمان را حفظ نمایند به تدریج جایگاه و اعتبارشان را از دست داده و دیگر نمی‌توانند موفق باشند. امنیت از دو عنصر اصلی تهدید و فرصت برخوردار است و برقراری امنیت منوط به رهایی نسبی از تهدیدها و بهره گیری مناسب از فرصت هاست(هزارجریبی و چرمی،۱۳۹۳). مهمترین مطلبی که در مورد امنیت باید مورد توجه قرار گیرد این است که بعد انسانی و رفتار انسانی در این مقوله مهم و حیاتی می‌باشد زیرا این انسان‌ها هستند که از سیستم‌ها و اطلاعات استفاده کرده و می‌توانند خواسته یا ناخواسته امنیت اطلاعات را زیر سوال ببرند. پرداختن به موضوع امنیت به عنوان یکی از عمده ترین شاخص های رفاه و توسعه ضروری می باشد(هزارجریبی و یاری،۱۳۹۱). امروزه اطلاعات عامل اصلی کسب قدرت است و تسلط واقعی، تسلط اطلاعاتی است. جنگ میان کشورهای غنی و فقیر در واقع جنگ اطلاعاتی است و کشورهای سلطه‌گر که خواستار استمرار بهره‌جویی خود از منابع و ثروت کشورهای عقب مانده هستند و علاقه‌ای به ایجاد زیربناهای اطلاعاتی در این کشورها ندارند. با توسعه و پیشرفت جوامع و علوم ارتباطی ، نحوه ارتکاب جرایم نیز از حالت ابتدایی خود فاصله گرفته است. انواع جرایم در فضای مجازی روزبه روز در حال گسترش بوده و کف خیابان برای ارتکاب جرم آرام آرام جای خود را به شبکه های رایانه ای می دهد و به فضای مجازی که هیچ گاه خورشید در آن غروب نمی کند و فضا همیشه روز است، منتقل می شود(وروایی و میرزکی،۱۳۹۰). نکته‌ی دیگری که باید به آن توجه کرد بروز جرایمی است که با پیشرفت تکنولوژی و پیچیده شدن جوامع انسانی شکل گرفته در حالی که در گذشته اصلا وجود نداشته است از جمله این جرایم می توان به جرایم سایبری و جرایم سازمان یافته و ... اشاره کرد. بسیاری از جرایم سازمان یافته با کمک تکنولوژی از جمله محیط سایبر دست به اقدامات مجرمانه در محیط ملی و فراملی می زنند. به طور کلی عبور از چالش های امنیتی نوین در عرصه جهانی مستلزم مبارزه با مصادیق جرایم سازمان یافته در عرصه ملی و فراملی است و برای مبارزه با آن، باید تدابیر و راهکارهای موثرتری را در سیستم قضایی و پلیس در نظر گرفت و آن را تقویت کرد(میلانی و باقری و مقدم،۱۳۹۵). مبارزه و پیشگیری از این جرایم نیازمند عزم و اراده جدی در سطوح حاکمیتی و ملی و نیز تدوین راهکارهای پیشگیرانه با استفاده از تمام ظرفیت-های فکری و پژوهشی نهادهای علمی، دانشگاهی، رسانه‌ای و نیز اندیشمندان جامعه است. از این رو، می‌توان پیشگیری از جرایم و برقراری امنیت را موضوعی سیستمی و جامعه بنیاد تلقی کرد(سردارنیا و شهربابکی،۱۳۹۷). مدیریت امنیت اطلاعات به دو بخش عمده فنی و مدیریتی تقسیم می شود که ادغام این دو جنبه کارایی امنیت اطلاعات را تضمین خواهد کرد (یانگ ،۲۰۱٤) لیکن برخی از پژوهشگران حوزه امنیت معتقدند طی سال‌های اخیر مسلم شده است که امنیت اطلاعات دیگر یک

موضوع فنی نیست، بلکه مسئله‌ای مدیریتی محسوب می‌شود (نادری،۱۳۹٦). در ایران در سال ۱۳۸٦ با بخشنامه معاون اول رئیس جمهور کلیه دستگاه‌های دولتی و غیردولتی موظف به تهیه طرح سیستم مدیریت امنیت اطلاعات شدند که سرمایه گذاری نسبتا زیادی را می‌طلبید اما با این وجود سازمان جهانی استاندارد (ISO) در سال ۲۰۱٤، رتبه ایران از نظر تعداد گواهینامه‌های اخذ شده در سیستم مدیریت امنیت اطلاعات را جایگاه ششم از میان چهارده کشور خاورمیانه اعلام نمود. آمار ارائه شده، نشان‌دهنده عدم توجه کافی در کشور به حوزه مدیریت امنیت اطلاعات می‌باشدکه به نظر می‌رسد نبود الگوی مناسب با دیدگاه همه جانبه نسبت به امنیت اطلاعات، توجه بیشتر به توسعه فنی این حوزه و عدم در نظر گرفتن جنبه مدیریتی آن سبب بروز این مشکل می‌باشد (عبدی، ۱۳۹۵) به همین دلیل با وجود توسعه و ایجاد راه‌کارها و تکنیک‌های پیچیده امنیتی شاهد وخیم‌تر شدن وضعیت امنیت اطلاعات در سازمان‌ها هستیم (عیدی،۱۳۹۷) و از طرفی با وجود برخی استانداردهای خارجی در حوزه مدیریت امنیت اطلاعات از جمله (NIST[۱]، COBIT[۲] و ISO۲۷۰۰۰[۳])، حرکت بر اساس سیستم مدیریت امنیت اطلاعات منطبق بر استانداردهای اروپایی که تطابق کمی با شرایط زیرساختی سازمان‌های ایرانی دارند دشوار به نظر می‌رسد (تقوا، ۱۳۹٦). پژوهش در حوزه امنیت اطلاعات شامل روش‌های فنی، رفتاری، مدیریتی، فلسفی و سازمانی می‌شود که به حفاظت از دارایی‌های اطلاعاتی موجود در سیستم می‌پردازد و تلاش می‌کند سازمان را همیشه روزآمد نگه دارد (کراسلر[٤]، ۲۰۱۳). هدف مدیریت امنیت اطلاعات در هر سازمان، حفظ سرمایه‌های سازمان (نرم افزاری، سخت افزاری، اطلاعاتی، ارتباطی و نیروی انسانی) است و برای دستیابی به این اهداف به الگوی منسجمی نیاز دارد (چین و وانگ[٥]، ۲۰۰۹). بر این اساس مسئله پژوهش حاضر کاوش الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته با استفاده از نظریه داده بنیاد می‌باشد که با هدف ارائه یک الگو در حوزه امنیت می‌کوشد تا از آسیب پذیری سازمان‌های دولتی کشور بکاهد.

۲- اهدف پژوهش

هدف غایی این پژوهش، خلق الگویی در خصوص مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته است. نظر به طرح نظام‌مند راهبرد پژوهشی نظریه‌پردازی داده بنیاد، اهداف پژوهشی بدین شرح می-باشند: ۱. کاوش عناصر تشکیل‌دهنده الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته(مقوله اصلی، شرایط علی، زمینه یا بستر، شرایط مداخله‌گر، راهبردهای کنش و واکنش متقابل و پیامدها) و نیز ارائه روابط میان آن‌ها ۲. معرفی الگوی مذکور.

از این‌رو پرسش پژوهش بدین‌گونه مطرح شد: الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته چگونه است؟

۳- چارچوب مفهومی پژوهش

---

[۱] National Institute of Standard and Technology (NIST)
[۲] Control Objective for Information and related Technology (CObIT)
[۳] International Standard Organization (ISO)
[٤] Crossler
[٥] Chin & wong

برای الگویابی مدیریت امنیت اطلاعات، لازم است ابتدا مفهوم اطلاعات، امنیت اطلاعات و مدیریت آن به درستی درک شده و عوامل موثر بر امنیت اطلاعات شناسایی شوند. بنابراین در این بخش به‌طور ویژه به مدیریت امنیت اطلاعات و مفاهیم مرتبط با پیشگیری از جرائم سازمان یافته پرداخته شده است.

۳-۱- مفهوم اطلاعات

اطلاعات یکی از منابع اصلی و با ارزش هر سازمان و یا ارگان دولتی یا خصوصی به حساب می‌آید. اهمیت اطلاعات در سازمان‌ها به حدی است که آن را به رگ‌های سازمان تشبیه نموده‌اند که عامل حیات بخش محسوب می‌شود و در صورت محدودیت یا به خطر افتادن این جریان، سازمان با مرگ مواجه خواهد شد. به هر حال اهمیت دادن به اطلاعات می‌تواند مزایای بسیاری برای سازمان در برداشته باشد و سهمی ضروری و اساسی در موفقیت سازمان در عرصه‌هایی چون نقدینگی و ارزش بازار داشته باشد. همچنین اطلاعات عامل پیوند دهنده سایر منابع سازمان است (پورتر و میلار[٦]، ۱۹۸۵).

۳-۲- امنیت اطلاعات

اندرس[۷] (۲۰۱٤) امنیت اطلاعات را به عنوان محافظت از سیستم‌های اطلاعاتی و اطلاعات در برابر دسترسی غیرمجاز، استفاده، افشا، اختلال، اصلاح و تخریب تعریف می‌کند.

ویتمن و ماتورد[۸] (۲۰۱۱) امنیت را به عنوان عاری بودن از خطر تعریف می‌کنند و امنیت اطلاعات را تنها یکی از چندین لایه امنیتی مورد نیاز مانند امنیتی فیزیکی، امنیت کارکنان، امنیت عملیات، امنیت ارتباطات و امنیت شبکه می‌دانند.

آپدگرو (۲۰۰۳) امنیت اطلاعات را حفظ محرمانگی، حفاظت اطلاعات از دسترسی‌های غیر مجاز، اطمینان از یکپارچگی، دقت و صحت اطلاعات و فراهم نمودن دسترسی به اطلاعات در هر زمان برای کاربران تعریف می‌کند. محققان بر این باور هستند که امنیت اطلاعات دارای سه ویژگی است که باید به آن‌ها توجه کرد. این سه ویژگی عبارتند از:

۱- امنیت اطلاعات یک مشکل فنی نیست بلکه یک مساله مدیریتی و کسب و کاری است (چانگ[۹] و همکاران، ۲۰۰٦).

۲- امنیت اطلاعات یک فرایند مدیریتی چرخشی تحت عنوان سیستم مدیریت امنیت اطلاعات است. در این فرایند مخاطرات به صورت پیوسته توسط کنترل‌های مناسب مدیریت می‌شوند. تا احتمال نتایج مخاطرات ناخواسته کاهش یابد (آرام، ۱۳۸۸).

۳- امنیت اطلاعات بر مبنای مدیریت مخاطرات بنا می‌شود. از آنجایی که به دست آوردن امنیت کامل، غیر قابل دسترس است همیشه یک سطح مخاطره برای امنیت اطلاعات باید در نظر گرفته شود. مخاطرات با کاهش احتمال وقوع آن‌ها یا با کاهش نتایج آن‌ها، تقلیل داده می‌شود (همان).

محققان ویژگی‌های متفاوتی را برای اطلاعات در نظر می‌گیرند. به عنوان مثال ویتمن و ماتورد (۲۰۱۳) محرمانه بودن[۱۰]، یکپارچگی[۱۱]، سودمندی[۱۲] و مالکیت[۱۳] را به عنوان ویژگی‌های مهم اطلاعات در نظر می‌گیرند در حالی که اندرس (۲۰۱٤)

---

[٦] Porter & Millar
[۷] Andress
[۸] Whitman & Mattord,
[۹] Chang

محرمانه بودن، یکپارچگی و در دسترس بودن[۱٤] را به عنوان مثلث CIA می‌پذیرد و مالکیت، اصالت (اعتبار)[۱۵] و سودمندی را به آن اضافه می‌کند.

مولفه‌های مثلث CIA به صورت زیر تعریف می‌شوند:

الف- محرمانه بودن: محرمانگی یعنی جلوگیری از افشای اطلاعات به افراد غیر مجاز یا جلوگیری از ازدست دادن آن‌ها (هومفریز[۱٦] و همکاران، ۱۹۹۸).

ب-یکپارچگی: یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها بطور غیرمجاز و تشخیص تغییر در صورت دستکاری غیر مجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات در حین انتقال بصورت غیر مجاز تغییر داده می‌شود (عاشوری زاده، ۱۳۹۱). سرویس یکپارچگی درست بودن اطلاعات را ارائه می‌کند.

پ- در دسترس بودن: اطلاعات باید زمانی که مورد نیاز افراد مجاز هستند در دسترس باشند. این ویژگی از آن‌رو مهم است که بدون آن فعالیت‌های معمول شرکت ادامه نمی‌یابد و تصمیمات به موقع گرفته نمی‌شود (گربر و وان سولمز[۱۷]، ۲۰۰۱).

به منظور حفظ امنیت اطلاعات، استانداردهای بین‌المللی وجود دارند که محرمانگی، یکپارچگی و در دسترس بودن اطلاعات را تضمین می‌کنند. این استانداردها در ادامه آورده شده‌اند.

۳-۳- استانداردهای امنیت اطلاعات

پور[۱۸] (۲۰۰۱) اظهار داشت که بدون استانداردهایی که معیارهای عینی را برای انتخاب امنیت اطلاعات فراهم کنند، مدیران ممکن است تصمیماتی را بر اساس فاکتورهای غیراصولی که ممکن است بر اساس سوگیری، محدودیت‌های درک شده و انگیزه‌های شخصی باشد، اتخاذ نماید. بنابراین استانداردهای بین‌المللی به وجود آمدند که جنبه‌های مختلف مدیریت اطلاعات را مورد بررسی قرار می‌دهند. در جدول ذیل این استانداردها شرح داده شده‌اند:

جدول ۱. استانداردهای امنیت اطلاعات

ردیف	استاندارد	توصیف	توضیح مختصر
۱	ISO/IEC ۲۷۰۰۲: ۲۰۰۵	کد عمل برای مدیریت امنیت اطلاعات	مشخصات: سیاست امنیتی، سازماندهی امنیت اطلاعات، مدیریت دارایی، امنیت منابع انسانی، امنیت فیزیکی و محیط زیست، مدیریت ارتباطات و عملیات، کنترل دسترسی، دستیابی به سیستم‌های اطلاعاتی، توسعه و نگهداری، مدیریت حوادث امنیتی اطلاعات، مدیریت پیوستگی تجارت،

[۱۰] Confidentiality
[۱۱] Confidentiality
[۱۲] Utility
[۱۳] Possession
[۱٤] Availability
[۱۵] Authenticity
[۱٦] Humphreys
[۱۷] Gerber & Von Solms
[۱۸] Poore

			انطباق.
	SO/IEC ۲۷۰۰۱:۲۰۰۵	الزامات سیستم مدیریت امنیت اطلاعات	الزامات مربوط به ایجاد، اجرا، بهره‌برداری، نظارت، بررسی، نگهداری و بهبود سیستم مدیریت امنیت اطلاعات را به طور مستند مشخص می‌کند. یک مدل چرخه‌ای معروف به «برنامه–اجرا–چک–اقدام» را معرفی می‌کند. اغلب همراه با ۲۰۰۵ :۲۷۰۰۲ ISO / IEC اجرا می‌شود.
۳	ISO/IEC ۱۵٤۰۸	معیارهای ارزیابی امنیت IT (معیارهای مشترک)	شامل سه بخش است که عبارتند از: معرفی و مدل کلی (۱۵٤۰۸–۱: ۲۰۰۵)، الزامات عملکردی امنیتی (۱۵٤۰۸–۲: ۲۰۰۵) و الزامات تضمین امنیتی (۳:۲۰۰۵ ۱۵٤۰۸). به ارزیابی، اعتبارسنجی و تأیید تضمین امنیت یک محصول فناوری در برابر عوامل مختلف کمک می‌کند. سخت‌افزار و نرم‌افزار را می‌توان در برابر این استاندارد ارزیابی کرد.
٤	صنعت کارت‌های پرداخت PCI / DSS	صنعت کارت پرداخت استاندارد امنیت داده‌ها	برای امنیت تراکنش با کارت اعتباری به صورت آنلاین
٥	COBIT	اهداف کنترلی برای اطلاعات و فناوری‌های مرتبط	چارچوبی که ابتکار عمل IT را با الزامات تجاری پیوند داده و شکاف بین الزامات کنترل، مسائل فنی و ریسک‌های تجاری را مشخص می‌کند.
٦	ITIL یا ISO/IEC سری ۲۰۰۰	اطلاعات فناوری لایبرری	در مورد فرآیندهای خدمات IT مشارکت دارد و نقش اصلی کاربر را در نظر می‌گیرد.

در هر حال باید توجه شود که هر استانداردی که انتخاب می‌شود باید برای آن سازمان، قابل پذیرش و کاربردی باشد.

۳–٤– مدیریت امنیت اطلاعات

مدیریت امنیت اطلاعات به فرایند ساختاری برای پیاده‌سازی و مدیریت مداوم امنیت اطلاعات در سازمان اشاره دارد (ورمولن و ون سولمز[۱۹]، ۲۰۰۲). امنیت اطلاعات به دلیل نقش مهم فناوری اطلاعات در شرکت‌ها، یکی از مولفه‌های اصلی در برنامه‌ریزی و مدیریت شرکت‌های مدرن است (نیانچاما و سوپ[۲۰]، ۲۰۰۱). نیانچاما و سوپ (۲۰۰۱) اشاره می‌کنند که سازمان‌ها علاوه بر پیچیدگی محیط سازمانی، با مدیریت امنیت اطلاعات و تکنولوژی‌های متنوع در مکان‌های مختلف و واحدهای مختلف سازمانی، روبرو هستند. کادام[۲۱] (۲۰۰۷) بیان می‌کند که اعتبار کل برنامه امنیت اطلاعات در یک سازمان متکی به یک سیاست امنیت اطلاعات است که به خوبی تدوین شده باشد. سیاست‌ها و رویه‌ها، دستورالعمل‌هایی را برای

[۱۹] Vermeulen & Von Solms
[۲۰] Nyanchama & Sop
[۲۱] Kadam

امنیت تکنیکی، فیزیکی و عملیاتی فراهم کرده و به این شکل امکان اینکه به موضوع امنیت به طور رسمی رسیدگی شود را فراهم می‌کند (ورمولن و ون سولمز، ۲۰۰۲). مارتین[۲۲] و همکاران (۲۰۱۱) معتقد هستند که به طور کلی یک سیستم مدیریت امنیت اطلاعات که همه جوانب و جزئیات را نظر گرفته باشد، به یک فضای اطلاعاتی ایمن منجر می‌شود که سیاست‌ها، معیارها، دستورالعمل‌ها، کدهای عملی (تکنولوژی، انسانی، اخلاقی، قانونی) را در نظر گرفته است. همه این مطالب، بیانگر این موضوع هستند که قرار دادن یک الگوی امنیتی قوی برای محافظت از منابع داخلی در برابر هکرها، کراکرها و سایر فریبکاران، کافی نیست مگر اینکه اعتبار و تایید کاربران وجود داشته باشد و بنابراین نیاز به مدیریت کاربر وجود دارد (کامویری، ۲۰۱۲). مطالعه پست و کاگان[۲۳] (۲۰۰٦) نشان داد که افزایش ارتباطات تیم امنیتی با کاربران، درک امنیتی را افزایش می‌دهد. البته نباید این ارتباط به حدی زیاد باشد که کاربران آن را به عنوان نوعی اختلال در کارشان تلقی نمایند.

همه آنچه تحت تدوین استراتژی، مدیریت کاربر، استفاده صحیح از ابزارها و غیره گفته شد در چارچوب مدیریت امنیت اطلاعات قرار می‌گیرد. بنابراین می‌توان گفت مدیریت امنیت اطلاعات بخشی از مدیریت اطلاعات است که وظیفه تعیین اهداف امنیت و بررسی موانع موجود برای رسیدن به این اهداف و ارائه راهکارهای لازم را بر عهده دارد. همچنین مدیریت امنیت وظیفه پیاده‌سازی و کنترل عملکرد سیستم امنیت سازمان را بر عهد داشته و در نهایت باید تلاش کند تا سیستم را همیشه روزآمد نگه دارد. هدف مدیریت امنیت اطلاعات در یک سازمان، حفظ سرمایه‌های سازمان (نرم‌افزاری، سخت‌افزاری، اطلاعاتی و ارتباطی و نیروی انسانی) در مقابل هرگونه تهدید (اعم از دسترسی غیر مجاز به اطلاعات، خطرات ناشی از محیط و سیستم و خطرات ایجاد شده از سوی کاربران) است (شفیعی نیک آبادی، ۱۳۹۰) و برای رسیدن به این هدف نیاز به یک برنامه منسجم دارد.

۳-۵- جرائم سازمان یافته

جرائم سازمان یافته به دلیل ویژگی خاص و آثار خطرناکی که در جامعه باقی می‌گذارد، در طول دهه های اخیر مورد توجه دست اندرکاران کنترل جرم قرار گرفته است. جرائم سازمان یافته عبارت از فعالیت های غیر قانونی و هماهنگ گروهی منسجم از اشخاص است که با تبانی با هم و برای تحصیل منافع مادی و قدرت، به ارتکاب مستمر مجرمانه شدید می پردازند و برای رسیدن به این هدف از هر نوع ابزار مجرمانه ای استفاده می کنند(وروایی و زندی،۱۳۹۸). دولت ها، سازمان های مجری قانون، محققان دانشگاه و صنعت امنیت سایبری بر این باورند که گروه‌های جرائم سازمان یافته بطور فزاینده ای درگیر جرائم دیجیتال شده اند. باید توجه داشت امروزه سازمان یافته ترین جرائم سایبری توسط تکنیسین های ماهری که دانش خود را در فعالیت های مجرمانه بکار می گیرند، ارتکاب می یابد(محمدی و مونس خواه،۱۳۹۵). توسعه و گسترش روزافزون فناوری‌های ارتباطی و اطلاعاتی نوین به ویژه در محیط سایبر و فضای مجازی است که همگام با دستاوردهای بی نظیر پلیسی، چالش‌های جدی و اساسی را برای مجموعه پلیس و واحدهای جرم یاب رقم زده است(طالبیان و ذولفقاری و دعاگویان و بتولی،۱۳۹۹). عصری که در آن زندگی می‌کنیم، عصر ارتباطات و انقلاب اطلاعات است. فناوری اطلاعات و ارتباطات در همه زوایای زندگی انسان نفوذ کرده و شیوه زندگی او را تغییر داده است. جنبش های اجتماعی امروزه بیشتر

[۲۲] Martin
[۲۳] Post & Kagan

متکی به تکنولوژی های جدید ارتباطی هستند و از فضای مجازی به عنوان سکویی برای فعالیت‌های کاملا مجازی شامل مخالفت های الکترونیکی مانند نافرمانی های مدنی، انگ‌زنی و.. استفاده می کنند(خواجه سروری و نیک نام،۱۳۹۱). پلیس به عنـوان نهـاد برقرارکننـدۀ نظم و امنیت اجتماعی و مسئول پیشگیری از وقوع جرم، نقش مؤثری در انجام تحقیقات مقدماتی اینگونه جرائم ایفا می‌کند. پلیس‌های آینده مجبور هستند قـانون را بـه وسـیلۀ مغزشان به اجرا بگذارند. فرآیند تحقیق، کشف و جمع‌آوری ادلـه در فضـای مجـازی بـر عهدۀ پلیس بوده و انجام این مراحل نیازمند دانش، ابزار و نیروهای متخصـص در زمینـۀ فناوری اطلاعات است(دلخون اصل و گلدوزیان و کلانتری،۱۳۹۸).

۳-٦- نقش عوامل انسانی در مدیریت امنیت اطلاعات

کارکنان نقش مهم در امنیت کلی اطلاعات در سازمان دارند. بدون در نظر گرفتن عامل انسانی، حتی ترفندهای فناوری نیز نمی‌تواند امنیت اطلاعات را تضمین نماید. سازمان‌ها به طور فزاینده از فناوری‌های امنیتی برای حفاظت از اطلاعات استفاده می‌کنند، اما امنیت اطلاعات تنها با استفاده از این فناوری‌ها حاصل نمی‌شود (هراث و رائو[۲٤]، ۲۰۰۹). امنیت اطلاعات موثر در سازمان‌ها به سه مولفه بستگی دارد: کارکنان، فرایندها و فناوری. تهدید امنیت داخلی به عنوان مجموعه اقدامات، رویدادها، موقعیت‌ها، حملات و حوادث داخل سازمان نه توسط افراد خارجی بلکه برای کاربران مجاز IT تعریف شده است. این نوع رفتارها را می‌توان به شرح زیر طبقه‌بندی کرد (آلیتی و آکایا[۲۵]، ۲۰۱۱):

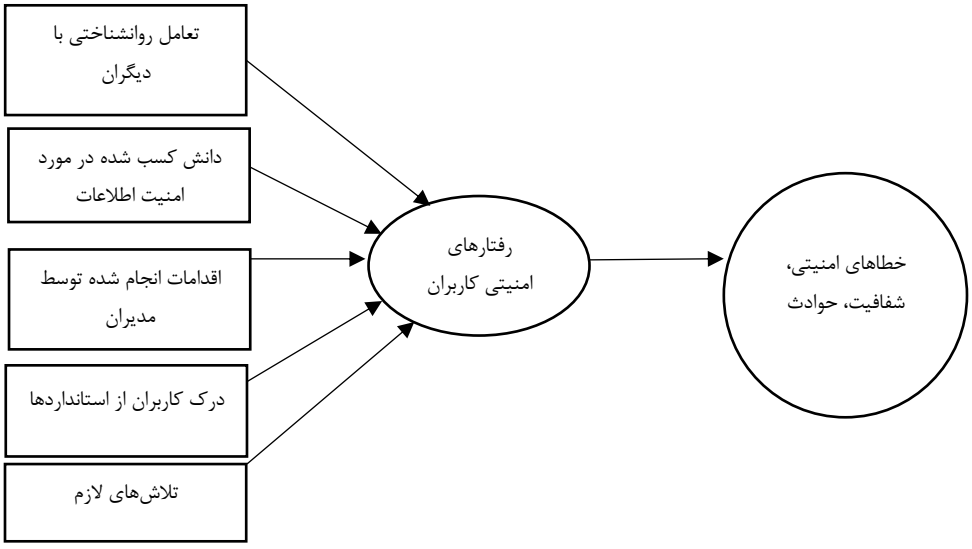
۱. عدم درک امنیت اطلاعات: اشتراک‌گذاری رمزهای عبور با دوستان، فراموش کردن اعمال مراحل امنیتی، عدم آگاهی از طرات وقایع در صورت بروز اشتباه.
۲. نادیده‌گیری: پذیرفتن سیاست‌های امنیتی بدون مطالعه آن‌ها.
۳. حملات: اقدامات عمدی به دلایل شخصی.
٤. خنثی سازی: سن کاربران بر رفتارهای امنیتی آن‌ها تاثیرگذار است. به عنوان مثال، جوانان با اعتماد به نفس بیشتری به سیستم‌های رایانه‌ای دارند. اما گاهی اوقات این اعتماد به نفس بیش از حد منجر به بروز رفتارهای ناایمن مانند خاموش کردن فایروال برای بارگیری پرونده می‌شود. همچنین معمولا افراد تمایل ندارند برای دریافت به روزرسانی، رایانه‌های خود را مجددا راه‌اندازی کنند و از عواقب امنیتی این عدم تمایل آگاهی کافی ندارند.
۵. پراگماتیسم[۲٦]: جوانان نسبت به نیازهای امنیتی عمل‌گرایانه‌تر هستند، آن‌ها ریسک‌های امنیتی را می‌دانند ولی در صورتی که دریافتی مناسبی داشته باشند حاضر هستند با این خطرات مواجه شوند.
٦. بی‌فایدگی[۲۷]: با وجود اینکه افراد به فناوری اعتماد دارند، اما همیشه یک احساس بیهودگی در ذهن آن‌ها وجود دارد. آن‌ها معتقد هستند همیشه متجاوزان روش‌های نفوذ خود را همگام با پیشرفت فناوری، ارتقا داده و حتی شاید یک قدم جلوتر باشند. بنابراین لازم است که به کارکنان نشان داده شود که همه چیز تحت کنترل است و دارایی‌ها امن هستند.

---

[۲٤] Herath and Rao
[۲۵] Aliti & Akkaya
[۲٦] Pragmatism
[۲۷] Futility

۷. قابلیت استفاده رابط‌های امنیتی: قابلیت استفاده نقش مهمی در مدیریت امنیت برای کارکنان دارد، زیرا پیاده‌سازی برخی رابط‌ها حتی برای متخصصین کامپیوتر پیچیده است، همچنین قابلیت استفاده از مکانیسم‌های امنیتی برای مدت طولانی مورد بررسی قرار می‌گیرد تا بتواند ابزارهای سازگار را طراحی کند.

لیچ[۲۸] (۲۰۰۳) معتقد است که درک افراد از مفهوم امنیت اطلاعات به مدیریت امنیت اطلاعات کمک می‌کند. شکل (۱) عوامل انسانی موثر بر امنیت اطلاعات را نشان می‌دهد.



شکل (۱): عوامل موثر بر رفتارهای امنیتی کاربران (لیچ، ۲۰۰۳)

بر اساس شکل (۱) اقدامات انسانی در قبال امنیت اطلاعات می‌تواند به شرح زیر باشد:

۱. آنچه به کارکنان گفته می‌شود
۲. آنچه کارکنان از دیگران می‌بینند و الگوبرداری می‌کنند.
۳. حس مشترک امنیتی و مهارت‌های تصمیم‌گیری کاربر

[۲۸] Leach

٤. ارزش‌های شخصی کاربر و استانداردهای رفتاری، احساس تعهد کاربر.

٥. دشواری اجرا

۳-۷- مدل‌های مختلف مدیریت امنیت اطلاعات

در تحقیقات انجام شده پیرامون مدیریت امنیت اطلاعات مدل‌های مختلفی تا کنون ارایه شده است که در ادامه به برخی از آن‌ها اشاره شده است.

الوف و ون سولمز[۲۹] یک چارچوب سلسله مراتبی را برای رویکردهای مختلف متشکل از سه سطح ارایه دادند، به‌طوری که سطح بالای آن، فناوری اطلاعات را به معنای وسیع خود نشان می‌دهد و کلیه فعالیت‌ها و ابزارهای مرتبط با آن و کلیه رویکردهای اتخاذ شده در IT را به طور کلی ارایه می‌دهد. این سطح از چارچوب همه دسته‌بندی‌های مرتبط با ارزیابی اطلاعات و فناوری‌های مرتبط با آن را پوشش می‌دهد. سطح دوم به دو بخش با نام‌های «فناری اطلاعات: عمومی» و «فناوری اطلاعات: امنیت» تقسیم می‌شود. حوزه «فناوری اطلاعات: عمومی» شامل کلیه فعالیت‌ها و ابزارهای فناوری اطلاعات است که نمی‌تواند خطرات امنیتی را متحمل شود. حوزه «فناوری اطلاعات: امنیت» خود به دو بخش فناوری و فرایندها تقسیم شده است. فرایندهای امنیتی به کلیه اقدامات مدیریت امنیت اطلاعات که باید انجام شود اختصاص داده می‌شود. و فناوری به کلیه جنبه‌های مشهود درگیر در امنیت فناوری اطلاعات، مانند کنترل‌هایی که برای جلوگیری از آسیب‌های احتمالی توسط نرم‌افزارهای مخرب در نظر گرفته شده است، می‌پردازد. در سطح سوم فرایندهای امنیتی به چهار سطح تقسیم می‌شوند که عبارتند از (۱) دستورالعمل‌ها، کدهای عملیاتی (۲) استانداردها (۳) قانون و (٤) معیار. فناوری امنیتی نیز دارای سطوحی مشابه با فرایندها است به جز قانون که با ارزیابی جایگزین می‌شود. در سطح پنجم، برخی از موارد ذکر شده در سطح قبل، به دو بخش داخلی و خارجی تقسیم می‌شوند. دستورالعمل‌های داخلی به طور خاص برای سازمان طراحی می‌شوند و دستورالعمل‌های خارجی، استانداردهای بین‌المللی هستند.

تروک[۳۰] (۲۰۰۳) چهارچوبی یکپارچه برای مدیریت امنیت سیستم‌های اطلاعاتی بر اساس چند صفحه لایه لایه پیشنهاد کرده است. وی معتقد است که برای حفاظت از اطلاعات، ابتدا باید تهدیدات مربوط به دارایی‌های کسب و کار، شناسایی شود. او بر اساس تجزیه و تحلیل تهدیدها، یک رویکرد چندلایه را پیشنهاد کرد. در پلن اول بر روی تعامل، تمرکز شده است. این پلن از مکانیسم‌های امنیتی شروع می‌شود و تا استقرار سرویس‌های امنیتی که انسان و ماشین را با یکدگیر پیوند می‌دهند ادامه می‌یابد. در نهایت، تعاملات انسانی باید پوشش داده شود. بنابراین به طور موازی، برای اجرایی کردن امور، پیشنهاد می‌کنند که به پلن‌های فناوری، سازمانی و قانون‌گذاری پرداخته شود.

٤- پیشینه پژوهش

٤-۱- تحقیقات داخلی

حدادی هرندی و همکاران (۱۳۹۸) به بررسی مدیریت امنیت اطلاعات در کسب و کار هوشمند پرداختند. نتایج نشان امنیت اطلاعات با هدف تضمین تداوم و به حداقل رساندن آسیب‌ها و تهدیدات سایبری، باعث حفظ و ارتقاء کسب و کار و به حداکثر رساندن فرصت‌های سرمایه‌گذاری از طریق توسعه بازارهای جدید می‌شود.

[۲۹] Eloff & von Solms
[۳۰] Trèek

دهقانی و همکاران (۱۳۹۸) به بررسی آگاهی، نگرش و عملکرد کارکنان بخش مدیریت اطلاعات سلامت بیمارستان‌های ایران نسبت به امنیت اطلاعات سلامت پرداختند. میانگین امتیازات آگاهی، نگرش و عملکرد شرکت‌کنندگان در زمینه مدیریت امنیت اطلاعات به ترتیب ۰/٦۷ ، ۳/۵۳ و ۱/٤۷ به دست آمده است. همچنین می‌توان با برگزاری دوره‌های آموزشی و ضمن خدمت، وضعیت امنیت اطلاعات سلامت در بیمارستان‌ها را ارتقا داد.

رضوانی، شهلا (۱۳۹۷) در پژوهشی با عنوان «طراحی الگوی مدیریت امنیت اطلاعات در کتابخانه‌های دیجیتالی» دریافت که سیستم‌ها و معماری‌های سازمانی و ممیزی کمک شایانی به استقرار سیستم‌های امنیت در سازمان‌ها خواهند نمود.

رضایی، علی و همکاران (۱۳۹۷) در پژوهشی با عنوان «عوامل موثر بر اثر بخشی سیستم مدیریت امنیت اطلاعات» دریافتند که شاخص‌های نقش مدیریت، آگاهی از سیستم امنیت اطلاعات و انطباق با آموزش، امنیت سیستم اطلاعات کسب و کار و ارزیابی ریسک امنیت سیستم اطلاعات بر اثربخشی سیستم مدیریت امنیت اطلاعات تاثیرگذار می‌باشد.

سیف و نادری بنی (۱۳۹٦) در پژوهشی به شناسایی مولفه‌های موثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران پرداختند. بر اساس نتایج این پژوهش، مولفه‌های مرتبط با مسائل فنی، انسانی، مدیریت و رهبری و نیز، مالی و اقتصادی موثر بر مدیریت امنیت اطلاعات واحد فناوری اطلاعات شرکت نفت فلات قاره ایران مشخص شدند.

خیرگو و شکوهی (۱۳۹٦) در پژوهشی با عنوان شناسایی و رتبه‌بندی عوامل کلیدی موثر بر اثربخشی سیستم‌های اطلاعاتی در سازمان‌های دولتی بیان کردند که امروزه سیستم‌های اطلاعاتی از عوامل موثر در دستیابی به مزیت رقابتی برای سازمان‌ها محسوب می‌شوند. چرا که کیفیت خروجی این سیستم‌ها نقش مهمی در بهبود عملکرد سازمان دارد. نتایج پژوهش آنها نشان دهنده تاثیر مثبت عوامل سازمانی، عوامل انسانی و فنی بر اثربخشی سیستم‌های اطلاعاتی است. همچنین، از بین شاخص‌های موثر بر اثربخشی سیستم‌های اطلاعاتی، حمایت مدیر ارشد، امنیت، پذیرش و مدیریت دانش فناوری اطلاعات و سیستم‌های اطلاعاتی، به ترتیب رتبه‌های نخست را به خود اختصاص داده‌اند.

٤-۲- تحقیقات خارجی

پارک[۳۱] و همکاران (۲۰۱۷)، نقش آموزش امنیت اطلاعات و عوامل فردی در افشای اطلاعات سلامت بیماران را بر گسترش امنیت اطلاعات بررسی کردند. یافته‌های این پژوهش نشان داد امنیت اطلاعات و ارزش‌های شخصی در آموزش پرستاری و و تلاش صنعت مراقبت‌های بهداشتی برای حفاظت از اطلاعات سلامت بیماران نقش جالب توجهی دارند.

وایگا و مارتینز[۳۲] (۲۰۱۷)، در پژوهش بهبود فرهنگ امنیتی اطلاعات از طریق اقدامات نظارت و پیاده‌سازی که بین ۵۱۲ نفر از کارکنان در آفریقای جنوبی انجام دادند، به این نتیجه رسیدند که ابزار ارزیابی فرهنگ امنیت اطلاعات می‌تواند در سازمان‌ها به طور موفقیت آمیزی بر فرهنک امنیت اطلاعات تاثیر بگذارد.

۵- روش‌شناسی پژوهش

جهت توصیف روش‌شناسی پژوهش لازم است پیاز (لایه‌های) تحقیق مشخص شود؛ لایه‌های پژوهش حاضر به شرح ذیل می‌باشد:

ازلحاظ فلسفه پژوهش: تفسیری (interpretive)

---

[۳۱] - Park
[۳۲] - Veiga. & Martins

از لحاظ جهت‌گیری‌های پژوهش: کاربردی (applied)

ازلحاظ رویکردهای پژوهش: استقرایی (inductive)

از لحاظ صبغه پژوهش: کیفی (qualified)

از لحاظ نوع پژوهش : اکتشافی (exploratory)

از لحاظ استراتژی : نظریه زمینه بنیاد (grounded theory)

از لحاظ هدف: کشف (explore)

از لحاظ شیوه گردآوری: مصاحبه (interview)

۵-۱- اجزاء پژوهش گراندد تئوری

داده‌ها: داده‌ها از طریق مصاحبه، مشاهده، اسناد و مدارک ، فیلم و ... جمع آوری می‌گردد.

کدگذاری: ترتیبات و گام‌های عملی برای تفسیر و سازمان دادن داده‌ها.

گزارش: گزارش‌های کتبی و شفاهی بصورت پایان‌نامه، مقاله، سخنرانی و ...

در تحقیق حاضر ترتیبات و گام‌های عملی با هدف شناسایی، پرورش و مربوط کردن مفاهیم با یکدیگر دنبال شده‌اند. از سوی‌دیگر با استفاده از نمونه‌گیری نظری، نمونه‌گیری در جریان پژوهش و مبتنی بر مفاهیم مستخرج از پژوهش، در حین پژوهش شکل گرفت و با نظریه در حال تکوین مرتبط شد. لذا مفاهیمی که در جریان تحلیل پدیدار شده‌اند شناسایی و مفاهیم مشابه در قالب یک مقوله نشان داده شد. از دیگر سو با پرسش‌های تحلیلی و مقایسه مداوم فرآیند گردآوری، داده‌ها هدایت شده و پرسش‌ها و مصاحبه شونده بعدی انتخاب گردید. فرآیند پژوهش به شرح ذیل جریان یافت. پس از مشخص نمودن، با استفاده از روش نمونه‌گیری خوشه‌ای و گلوله برفی گروه مورد مصاحبه و پرسش شناسایی می‌گردد. سپس اقدام به مصاحبه می‌گردد. در این پژوهش هدف، دریافت نظر خبرگان در خصوص شناسایی راهبردهای مدیریت امنیت اطلاعات در سازمان-های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته است. مصاحبه‌ها ساختار نیافته و دارای رویکردی اکتشافی است. برای تحلیل مصاحبه بر اساس نظریه زمینه‌ای از کدگذاری باز، کدگذاری محوری و کدگذاری گزینشی استفاده می شود.

دوره‌های زمانی انجام تحقیق : دوره زمانی تحقیق سال‌های ۱۳۹۸ و ۱۳۹۹ است.

مکان تحقیق : مکان تحقیق کشور ایران می‌باشد.

۵-۲- نمونه‌گیری

نظریه زمینه بنیاد مانند دیگر روش‌های کمی و کیفی متکی بر تصورات معرف بودن نمونه آماری برای تعمیم پذیری داده‌ها و اصالت یافته‌ها نیست و عموما نمونه ها بصورت هدفمند انتخاب می‌شوند. در این تحقیق از روش نمونه‌گیری نظری استفاده شده است. در این روش نمونه‌گیری جمع‌آوری داده‌های مداوم برای خلق نظریه در جریان است. بگونه‌ای که تحلیل قبلی بر نحوه تصمیم‌گیری در مورد اینکه چه داده‌هایی باید جمع‌آوری شود تاثیرگذار است بعبارت دیگر جمع‌آوری و تحلیل داده بصورت همزمان انجام می‌شود (مقایسه‌ی پیوسته‌ی داده‌ها). نمونه‌گیری نظری یکی از ویژگی‌های اساسی نظریه‌پردازی زمینه بنیاد است. با توجه به هدف پژوهش از روش نمونه‌گیری گلوله برفی یا زنجیره‌ای استفاده شد. در واقع در اشباع نظری الف) هیچ داده جدید یا مرتبط به یک مقوله به دست نمی‌آید ب) مقوله از لحاظ ویژگی‌ها و ابعاد به خوبی پرورش یافته و

گوناگونی‌های آن را به نمایش گذاشته باشد ج) مناسبات میان مقوله‌ها به خوبی مشخص و اعتبارشان ثابت شده باشد. که در پژوهش حاضر با ۱۷مصاحبه به این موقعیت دست یافتیم.

٦- فرآیند اجرائی تحقیق

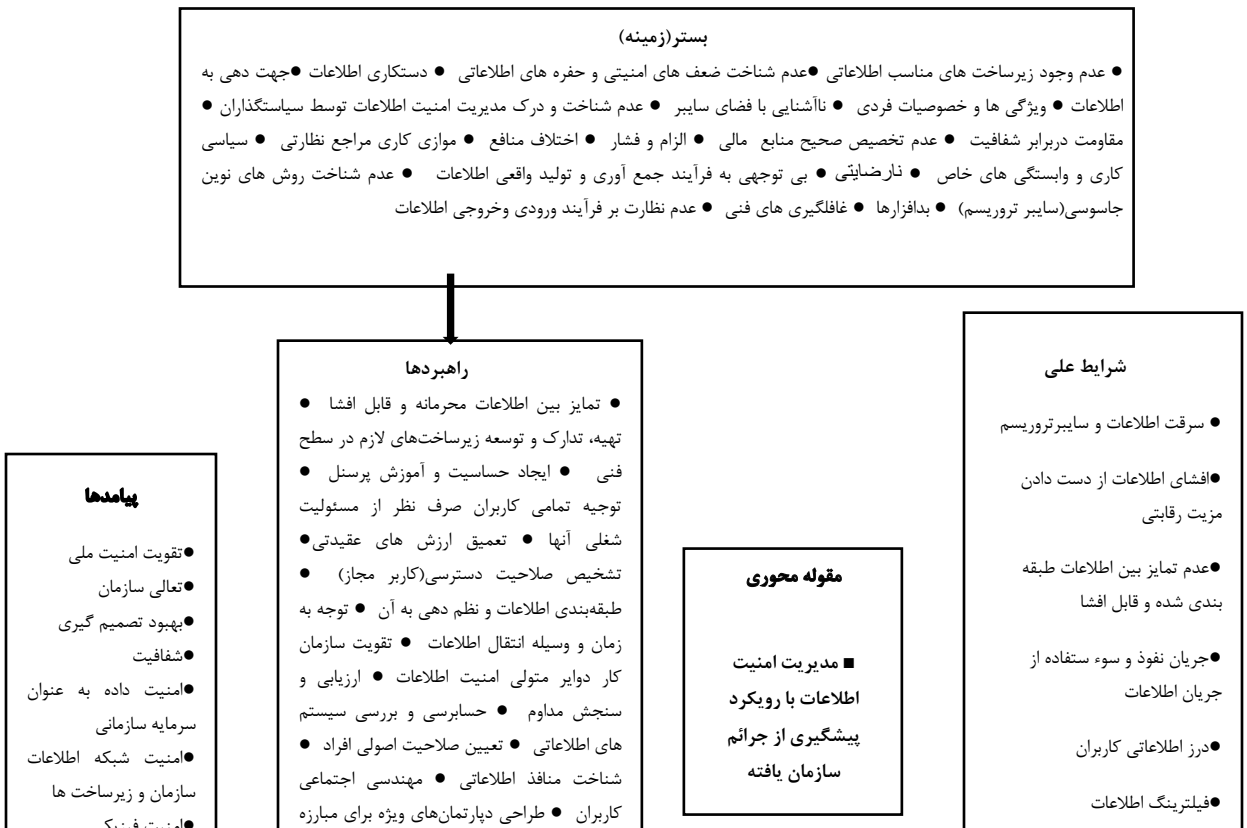
الف) طراحی ساختار مصاحبه و انجام آن: ابتدا ساختار سوالات اولیه مصاحبه جهت شروع طراحی و اولین مصاحبه شروع شد که سوالات مصاحبه باز و مصاحبه شونده دارای آزادی عمل در پیشبرد موضوع گردید اما جریان مصاحبه تحت کنترل مصاحبه‌گر قرار داشت. پس از خاتمه هر مصاحبه مطالب ضبط شده از هر مصاحبه، پیاده سازی و مدل اولیه هر مصاحبه استخراج و با مدل مصاحبه های قبلی مقایسه می‌شد.

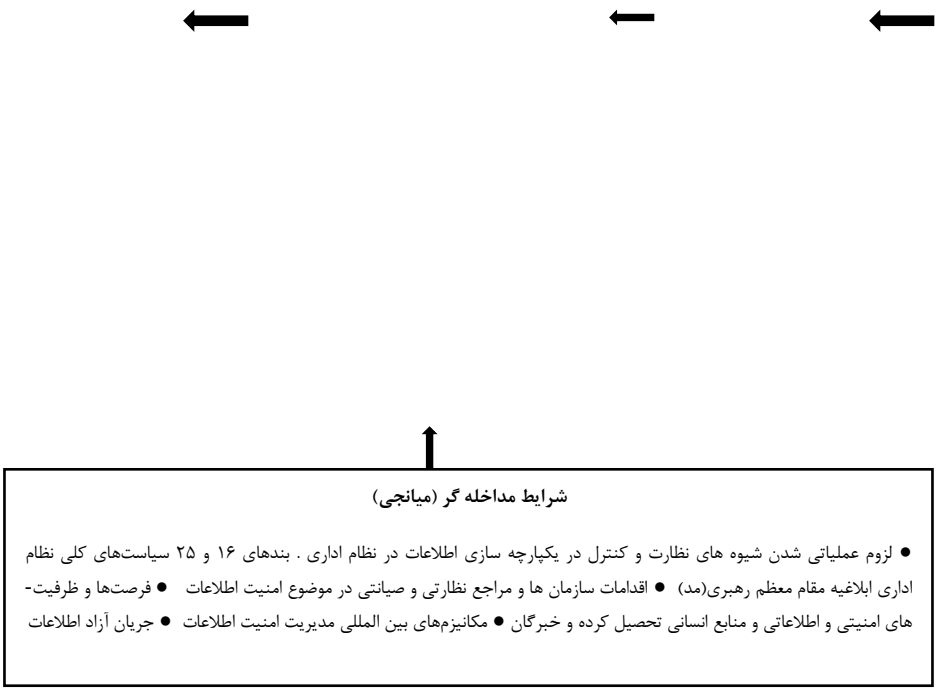
ب) استخراج مقوله‌ها و مفاهیم: با استفاده از کدگذاری باز مفهوم‌ها شناسائی و ویژگی‌ها و ابعاد آن در داده‌ها کشف و پس از آن از طریق مفاهیم مشابه مقوله‌ها ساخته شد. در واقع پدیده‌ها ایده‌های مرکزی در داده‌ها هستند که بصورت مفهوم نمایان می‌شوند. مفهوم‌ها بنای نظریه را تشکیل می‌دهند و مقوله‌ها مفهوم‌هایی هستند که معنای پدیده‌ها را می‌رسانند. این عمل تا آنجا ادامه یافت تا اشباع نظری حاصل گردد. اشباع نظری نقطه‌ای است ویژگی/ ابعاد/ روابط جدید حاصل نشود.

ج) ارتباط بین مقوله‌ها: به کمک کدگذاری محوری مقوله‌ها به مقوله‌های فرعی و مفاهیم مرتبط شد و مقوله‌ها در سطح ویژگی‌ها و ابعاد با یکدیگر نیز مرتبط شدند. پس از آن ساختار مقوله از طریق شناسایی بستر یا زمینه‌ای که مقوله در آن قرار دارد صورت گرفت.

د) پالایش نظریه و تدوین مدل نهائی پژوهش: با استفاده از کدگذاری گزینشی، یکپارچه‌سازی و پالایش نظریه انجام شد. در نهایت مدل مفهومی پژوهش استخراج گردید:

" الگوی مدیریت امنیت اطلاعات در سازمان های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته "





۷- یافته‌های پژوهش و نتیجه‌گیری

در روش نظریه‌پردازی داده بنیاد پاسخ به پرسش پژوهش، همان الگوی بدست آمده و عناصر آن می‌باشـــد. در حقیقت، یافته-های پژوهش؛ مقوله ها و مؤلفه های آن می باشند که در این پژوهش، در قالب الگو بیان شـــده‌اند. در راستای نیل به اهداف و نیز پاســـخ به پرســـش پژوهش، پس از اجرای راهبرد پژوهشـــی کیفی داده بنیاد، الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته با اجزای آن استخراج گردید که به اختصار بیان می‌گردند. از آن‌جا که در روش داده بنیاد، نظریه جدیدی بوجود آمده است لذا همه یافته‌ها قابل مقایســـه با ادبیات پیشین نبوده و برای بررسی کامل، بایستی در پژوهش‌های آتی مورد بررسی کمی و ارزیابی قرار گیرند. الگوی مدیریت امنیت اطلاعات با رویکرد پیشگیری از جرائم سازمان یافته دارای مزایای مختلفی از قبیل تقویت امنیت ملی، تعالی سازمان، بهبود تصمیم‌گیری، شفافیت، امنیت داده به عنوان سرمایه سازمانی، امنیت شبکه اطلاعات سازمان و زیرساخت ها، امنیت فیزیکی و برقراری عدالت اجتماعی است. این امر میسر نمی‌شود مگر اینکه قبل از آن مدیریت امنیت اطلاعات مورد پذیرش واقع شود. پذیرش این مهم نیز مستلزم شناسایی موانع و مشکلات آن و در نهایت شناسایی راهبردهایی برای پذیرش و بکارگیری آن است. لذا ابتدا موانع و مسائل و سپس راهبردهای متناسب با آنها شناسائی شد، که در ادامه بیان می‌گردد. موانع و مسائل شناسایی شده عبارتند از: عدم وجود زیرساخت‌های مناسب اطلاعاتی، عدم شناخت ضعف‌های امنیتی و حفره های اطلاعاتی، دستکاری اطلاعات، جهت دهی به اطلاعات، ویژگی ها و خصوصیات فردی، ناآشنایی با فضای سایبر، عدم شناخت و درک مدیریت امنیت اطلاعات توسط سیاستگذاران، مقاومت در برابر شفافیت، عدم تخصیص صحیح منابع مالی، الزام و فشار، اختلاف منافع، موازی کاری مراجع نظارتی، سیاسی کاری و وابستگی‌های خاص، بی توجهی به فرآیند جمع‌آوری و تولید واقعی اطلاعات، عدم شناخت روش‌های نوین جاسوسی (سایبر تروریسم)، بدافزارها، غافلگیری‌های فنی و عدم نظارت بر فرآیند ورودی و خروجی اطلاعات می‌باشند بنابراین ضرورت دارد راهبردهائی جهت رفع این موانع شناسایی و بکار بسته شود. در این

پژوهش جهت رفع، موانع راهبردهای: تمایز بین اطلاعات محرمانه و قابل افشا، تهیه، تدارک و توسعه زیرساخت‌های لازم در سطح فنی، ایجاد حساسیت و آموزش پرسنل، توجیه تمامی کاربران صرف نظر از مسئولیت شغلی آنها، تعمیق ارزش‌های عقیدتی، تشخیص صلاحیت دسترسی (کاربر مجاز)، طبقه‌بندی اطلاعات و نظم‌دهی به آن، توجه به زمان و وسیله انتقال اطلاعات، تقویت سازمان کار دوایر متولی امنیت اطلاعات، ارزیابی و سنجش مداوم، حسابرسی و بررسی سیستم‌های اطلاعاتی، تعیین صلاحیت اصولی افراد، شناخت منافذ اطلاعاتی، مهندسی اجتماعی کاربران، طراحی دپارتمان‌های ویژه برای مبارزه با سایبر تروریسم، اشرافیت اطلاعاتی، کنترل ورودی و خروجی اطلاعات و فراگیر شدن دولت الکترونیک (شفاف-سازی فرآیندها) شناسایی شد. البته هر کدام از این راهبردها نیز نیازمند برنامه استراتژیک خاص خود است به عنوان مثال جهت پیشبرد راهبرد تمایز بین اطلاعات محرمانه و قابل افشا باید تعریف دقیقی از اطلاعات محرمانه و طبقه‌بندی شده در سازمان ارائه شده و مواردی که از قید محرمانگی مستثنی هستند نیز مشخص شوند. تهیه و توسعه زیرساخت‌های فنی امنیت اطلاعات نیز به عنوان یکی دیگر از راهبردهای مشهود در مدل، می‌تواند با انجام مشاوره‌های علمی و فنی با صاحبان دانش فناوری اطلاعات و ارتباطات پس از بکارگیری ابزارها و لوازم مختلف اطلاعاتی و ارتباطی با دیدی روشن و کامل از نیازهای سازمان در راستای تامین امنیت اطلاعات در سازمان‌های دولتی اثرگذار باشد. در خصوص راهبرد تعمیق ارزش های عقیدتی، یکی از عواملی که افراد را از بزهکاری باز می دارد، رعایت تعالیم مذهبی و داشتن ارتباط با خداوند است، به همین دلیل است که در ماه هایی مثل ماه محرم و ماه رمضان شاهد کاهش آمار وقوع جرم در جامعه هستیم(وروایی،۱۳۸۷). با توجه به گستردگی جرائم سازمان یافته و همچنین آثار مخرب و گسترده این جرائم، کنترل جرائم سازمان یافته و پیشگیری از تکرار این جرائم کاملا ضروری است. بنابراین با تدوین استراتژی‌های مناسب جهت رفع موانع یاد شده در الگوی فوق می‌توان امیدوار بود که الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی ایران با رویکرد پیشگیری از جرائم سازمان یافته پذیرفته و بکار گرفته شود. یافته‌های بدست آمده در تحقیق حاضر و نظریات مطرح شده در ابتدای پژوهش، درستی الگوی بدست آمده در چارچوب مدیریت امنیت اطلاعات را تقویت می‌کند. با توجه به این که پژوهش حاضر با استفاده از روش داده بنیاد، نظریه جدیدی را معرفی نموده است، توصیه می‌شود عناصر آن به طور کمی مورد بررسی قرار گرفته و با نظریات موجود مقایسه شوند.

۸- پیشنهادات کاربردی

توجه جدی تصمیم‌گیران و سیاست‌گذاران کشور به حوزه مدیریت امنیت اطلاعات به عنوان یکی از راهبردهای مهم اجرایی مدیریت اطلاعات

با شناسایی عوامل زمینه ای مدیریت امنیت اطلاعات در این پژوهش، مقتضی است خط‌مشی گذاران و تصمیم‌گیران و مدیران کشور در راستای اجرایی شدن این عوامل برنامه‌ریزی نمایند.

با شناسایی عوامل زمینه‌ای شکل‌گیری کارافرینی دانش بنیان در این پژوهش، مقتضی است خط‌مشی‌گذاران و تصمیم-گیران و مدیران کشور در راستای اجرایی شدن این عوامل برنامه‌ریزی نمایند.

برنامه‌های حمایتی جهت پذیرش و اجرای داوطلبانه الگوی مدیریت امنیت اطلاعات در سازمان‌های دولتی توسط مراجع متولی تدارک دیده شود.

با عنایت به اینکه مدیریت امنیت اطلاعات را می‌توان از منظر اسلام و منابع دینی و اندیشـــه رهبران اسلامی مورد توجه قرار داد، پیشنهاد می‌شود این پدیده طی مطالعاتی جداگانه و در چارچوب روش‌شناسی دینی مورد پژوهش واقع شود.

با توجه به گزاره‌های حکمی مســـتخرج از دل نظریهٔ داده بنیاد صورت‌بندی شـــده در پژوهش، توصیه می‌شود پژوهش‌هایی کمی با هدف آزمون این فرضیه‌ها انجام شوند.

با استفاده از روش‌های کمی، روابط بین همه مقوله‌ها و میزان وابستگی بین آن‌ها مورد بررسی قرار گیرد.

منابع

آرام، محمدرضا "بررسی و سنجش مولفه‌های موثر بر مدیریت امنیت اطلاعات شرکت گاز پارس جنوبی"، پایان نامه کارشناسی ارشد دانشگاه شهید بهشتی، (۱۳۸۸).

تاج فر، امیرهوشنگ "رتبه‌بندی موانع پیاده‌سازی سیستم مدیریت امنیت اطلاعات و بررسی میزان آمادگی مدیریت اکتشاف، journal of information technology management، ۲۱ (۱۳۹۳) ٥٦٦-٥٥١.

تقوا، محمدرضا "مدل پیاده‌سازی مدیریت امنیت فناوری اطلاعات در صنعت بانک‌داری ایران"، *فصلنامه مدیریت فناوری اطلاعات*، دوره ۹. شماره ۲. (۱۳۹٦) ٤٠٤-۳۷۹.

حدادی هرندی، علی اکبر؛ والمحمدی، چنگیز؛ صالحی صدقیانی، جمشید "مدیریت امنیت اطلاعات در کسب و کار هوشمند"، *علمی پژوهشی مدیریت بحران (ویژه‌نامه هوشمند سازی)*، ۸ (۱۳۹۸) ۲۵-۳۳

خواجه سروری، غلامرضا، خجسته، کمیل "الگوی رقابت رسانه ای جبهه انقلاب اسلامی با جبهه غربی در فتنه ۸۸ با محوریت فضای مجازی"، *فصلنامه اسلام و مطالعات اجتماعی*، ۷(۱)، (۱۳۹۸)، ۱۷٤-۱٤٤

خواجه سروری، غلامرضا، نیک نام، رضا، خلیل پور، علی، یزدانپناه، مهدی "تاثیر توسعه فناوری های اطلاعاتی و ارتباطی بر تحولات جدید خاورمیانه"، *فصلنامه رسانه*، ۲۳(۲)، (۱۳۹۱)

دلخون اصل، رامین، گلدوزیان، ایرج، کلانتری، کیومرث " نقـش پلـیس در جمـع آوری ادلـۀ الکترونیکی در فضای مجازی در نظام حقوقی ایران ، فرانسه و کنوانسیون جرائم سایبری"، *فصـلنامۀ پـژوهش هـای اطلاعاتی و جنایی* ،(٥٤)١٤، ۱۳۱-١٤٨

ذوالفقاری، حسین، طالبیان، حسین، دعاگویان، داود، بتولی، سیدحسن " نظام جامع جرم یابی در پلیس ایران" ، *فصلنامه پژوهش های اطلاعاتی و جنایی*، ۱۵(۵۸)، (۱۳۹۹)، ۱۱٤-۸۹

سردارنیا، خلیل اله، شهربابکی، میرزا مهدی " واکاوی پیشگیری از جرایم در ایران با تمرکز بر نظریۀ سیستمی در علوم سیاسی"، *فصلنامه پژوهش حقوق کیفری*، ۷(۲۷)، (۱۳۹۸)، ۷۳-٤۳

شفیعی نیک آبادی، محسن "مدلی برای مدیریت دانش جهت بهبود عملکرد زنجیره تامین در صنعت خودروسازی ایران"، پایان نامه دکترای دانشگاه علامه طباطبایی (۱۳۹۰).

شمس، شهاب الدین؛ اسفندیاری مقدم، امیر "ارتباط ابعاد مختلف اعتماد سازمانی با رضایت شغلی کارکنان"، *مطالعات مدیریت (بهبود و تحول)*، سال بیست و سوم، شماره ۷۷، (۱۳۹٤) صفحات ۱۷۱- ۱۸۵.

عاشوری زاده، سهیلا "رابطه فرهنگ سازمانی با مدیریت امنیت اطلاعات در بانک ملی ایران"، پایان نامه کارشناسی ارشد. دانشگاه علامه طباطبایی (۱۳۹۱).

عبدی، بهنام "ارائه مدلی برای امنیت اطلاعات با رویکرد مدیریت استراتژیک فناوری اطلاعات،" *کنفرانس بین المللی پژوهش های کاربردی در مدیریت و حسابداری"*، دوره٤، دانشگاه شهید بهشتی (۱۳۹۵).

عیدی، فاطمه،" بررسی تاثیر تهدیدات امنیت اطلاعات بر افشای اطلاعات شخصی (مطالعه موردی: کاربران اینترنت در دانشگاه پیام نور البرز)"،*سومین کنفرانس ملی فناوری در مهندسی برق و کامپیوتر*،سمنان (۱۳۹۷).

محمدی، سهیلا، مونس خواه، عیسی، " ماهیت گروه های سازمان یافته جرایم سایبری"، *فصلنامه علمی – ترویجی پژوهش های حقوقی*، ٤٠ (۱۳۹۸)، ۲۱۱-۱۸۹

محمدی، مهین؛ شیخ ظاهری، عباس؛ کرمانی، فرزانه "مقایسه الگوریتم‌های بیمار محور برای امنیت اطلاعات سلامت در شبکه‌های اجتماعی سلامت و محیط ابر"، *مجله اطلاع‌رسانی پزشکی نوین*، دوره پنجم، شماره دوم، (۱۳۹۸) صص۶۸-۷۹.

میلانی، علیرضا، باقری، نفیسه، مقدم، محمد مهدی "عملکرد نظام حقوقی ایران در مواجهه با جرائم سازمان یافته"، *فصلنامه مطالعات علوم اجتماعی*،۲، (۱۳۹۵)، ۱۱-۱

موسوی، پریسا، حسن‌پور، اکبر "شناسایی ریسک‌های امنیت اطلاعات سازمانی با استفاده از روش دلفی فازی در صنعت بانک‌داری"، *فصلنامه مدیریت فناوری اطلاعات*، ۱ (۷)، (۱۳۹٤) ۱۸٤-۱٦۳.

میوالد، اریک "مبانی امنیت شبکه. ترجمه: گروه پژوهشی فناوری اطلاعات جهاد دانشگاهی صنعتی شریف "تهران: انتشارات انستیتو ایز ایران (۱۳۸۵).

نادری، ناهید "شناسایی مولفه های موثر بر مدیریت امنیت اطلاعات در فناوری اطلاعات شرکت نفت فلات قاره ایران"، *فصلنامه مدیریت فناوری اطلاعات*،٤ (۹)، (۱۳۹٦) ۸۷۰ – ۸۵۱.

وروایی، اکبر" نقش فرماندهان و مدیران در راهبرد سازمانی صیانت از کارکنان"، *فصلنامه نظارت و بازرسی*، شماره ٦، (۱۳۸۷) ۱۲۸-۱۱۱.

وروایی، اکبر، زندی، مردان "سیاست کیفری تقنینی در پیشگیری از جرائم سازمان یافته"، *فصلنامه پژوهش های اطلاعاتی و جنایی*، ۱٤(٥٦)،(۱۳۹۸)، ۹٤-۷۹

وروایی، اکبر، میرزکی، سید شمس الدین " بررسی عوامل مؤثر بر کشف جرم کلاهبرداری رایانه ای پلیس آگاهی تهران"، *فصلنامه کاراگاه*، ۲ (٤)، (۱۳۹۰) ۸۷-٦۲

هزارجریبی، جعفر، چرمی، مصطفی، فاروقی، الهام، متقدم، عقیل "بررسی میزان احساس امنیت اجتماعی و عوامل موثر بر آن (مطالعه موردی شهر تهران)"، *فصلنامه برنامه ریزی رفاه و توسعه اجتماعی*، شماره ۲۰، (۱۳۹۳)

هزارجریبی، جعفر، یاری، حامد "بررسی رابطه احساس امنیت و اعتماد اجتماعی در میان شهروندان"، *پژوهش های راهبردی امنیت و نظم اجتماعی*، ۱ (٤)،(۱۳۹۱) ٥۸-۳۹

یوسفی، سجاد؛ مرادی، مرتضی؛ تیشه ورزدائم، محمد کاظم "نقش تعهد سازمانی کارکنان در تسهیم دانش"، *توسعه انسانی پلیس*، ۷ (۳۰) (۱۳۸۷) ۲٤ -۳٦.

Andress, J. The basics of information security: understanding the fundamentals of InfoSec in theory and practice. Syngress.(٢٠١٤).

Chang. E. An Investigation of Organizational Culture on Information Security Management. *Academy of Management Journal*, ٣٥, (٢٠٠٧).

Heidari, S., & Mohammadi, S. A New Model for Information Security Management in Service-Oriented Enterprise Architecture. *American Journal of Scientific Research*, (٧٦), (٢٠١٢), ١١٤-١٣٢.

Herath, T., & Rao, H. R. Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, ٤٧ (٢), (٢٠٠٩),١٥٤-١٦٥.

Kadam, A. W. Information security policy development and implementation. Information Systems Security, ١٦ (٥), (٢٠٠٧), ٢٤٦-٢٥٦.

Kambwiri, LAn Appraisal of Information Security Management at Chancellor College, University of Malawi., (٢٠١٢).

Nyanchama, M., & Sop, P. Enterprise security management: *Managing complexity. Inf. Secur. J. A Glob. Perspect*., ٩ (٦), (٢٠٠١), ١-٨.

Poore, R. S. Information Security Standards: Deluge and Dearth. *Inf. Secur. J. A Glob. Perspect*., ١٠ (١), (٢٠٠١) ١-٦.

Trèek, D. An integral framework for information systems security management. Computers & Security, ٢٢ (٤) (٢٠٠٣), ٣٣٧-٣٦٠.

Vermeulen, C., & Von Solms, R.. The information security management toolbox–taking the pain out of security management. *Information management & computer security*, (٢٠٠٢).

Whitman, M. E., & Mattord, H. J. Principles of information security. *Chengage Learning*, (٢٠١١).